HACKER JOURNAL

Anno 2 – N. 26
22 Maggio - 5 Giugno 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it,

Contributors: DaMè, Boymix81, Antonino Benfante, Roberto "decOder" Enea, Nicola D'Agostino, Paolo Iorio, RoSwEIL, 3d0, Lidia, Il Coccia

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Immagine di copertina: Daniele Festa

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

FATTA LA LEGGE, TROVATO L'HACK

Immaginate il vostro parco preferito. Quello dove, nelle domeniche di sole, andata con gli amici, la ragazza (o il ragazzo), una palla e la chitarra. È un parco pubblico, aperto a tutti, e avete tutti i diritti di andarci ogni volta che volete.

Ora immaginate che, un brutto giorno, andate al parco e scoprite che –durante la notte– qualcuno lo ha recintato e ha messo un cancello chiuso a chiave. Nessuno ha cambiato la legge o la proprietà del parco: è sempre un parco pubblico, e continuate ad avere il diritto di entrare e restare per tutto il tempo che volete. Solo che qualcuno lo ha imprigionato in una gabbia di ferro.

Fortunatamente, nessuno vi punirà se scavalcherete il recinto, o se forzerete la serratura. Ma se solo provate a vendere o regalare una chiave che possa aprire il cancello, rischierete la prigione. In questo modo, solo i più "giovani e forti", oppure chi avrà le capacità tecniche per forzare la serratura, potrà effettivamente esercitare il suo legittimo diritto a entrare nel parco.



Un meccanismo del genere sembra partorito dal genio di Kafka, e invece è frutto delle meningi dei nostri parlamentari. Già, perché se sostituite l'immagine del parco con quella del diritto alla copia personale di musica e video, e anziché immaginare una serratura meccanica pensate a una chiave di protezione hardware o software, la situazione descritta qui si applica perfettamente alla copia dei CD audio.

Il Decreto Legislativo n.68/03 del 09 aprile 2003, in vigore dal 29 aprile scorso, stabilisce infatti la legittimità delle misure anti copia messe in atto dai produttori cinematografici e musicali, e punisce chiunque "fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti [...] principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure (anti copia, NdR)".

Tutto ciò nonostante rimanga in vigore il diritto alla copia personale. Il Decreto Legislativo anzi ribadisce che i produttori devono consentire l'esercizio del diritto alla copia. Il trucco è che, per la legge, è sufficiente che si possa effettuare una copia solo analogica. Tutto ciò in un periodo in cui le autoradio a cassette vengono rimpiazzate da quelle con lettore di CD, e in cui il walkman sta cedendo il passo ai lettori di Mp3 portatili.

Cosa si può fare? Visto che la diffusione delle informazioni ancora non è reato, da parte nostra abbiamo deciso di pubblicare in questo numero una guida su come superare le protezioni anti copia per i CD audio, e stiamo preparando una sintesi ragionata della legge, per spiegare con parole chiare che cosa si può fare, cosa è vietato, e cosa si rischia in caso di infrazione (la troverete sul prossimo numero).

grand@hackerjournal.it

www.hackerjournal.it

Saremo di nuovo in edicola Giovedì 22 maggio!



STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

HACKER JOURNAL

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

NOTIZIE IN TEMPO REALE



**L'ipetrattivo Bismark, in collaborazione con Security Flop, ha aggiunto alla home page del sito di Hacker Journal un box con notizie su sicurezza e informatica, continuamente aggiornate.
Altro che ANSA...**

I MIGLIORI DIECI

Ecco la classifica dei dieci autori di messaggi più prolifici del nostro forum. Lodi e applausi da parte della redazione; e se hanno risposto a qualche vostro messaggio, risolvendovi un problema, non dimenticate di ringraziarli...

NOME	MESSAGGI
alt_os	251
Onscureravan	130
Z3n0	117
Lord_Dex	105
Doctormk	103
Milo_Cutty	94
Neuromante	92
tracciazero	84
bigthistle	65
Carmageddon	61

I NOSTRI/VOSTRI BANNER!

Volete mettere un banner di HJ sul vostro sito? Ne avete ben 120 tra cui scegliere! Avete fatt o un banner? Mandatelo all'indirizzo:

banner@hackerjournal.it

Lo pubblicheremo insieme agli altri.



Krakus



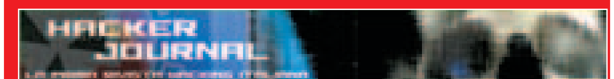
basher



697



Spyro



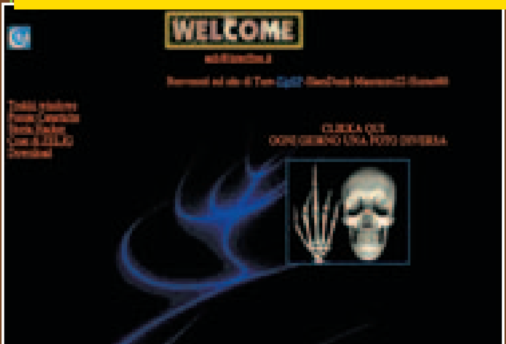
Norton

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: es3me
pass: assi2

Dai bit alla carta



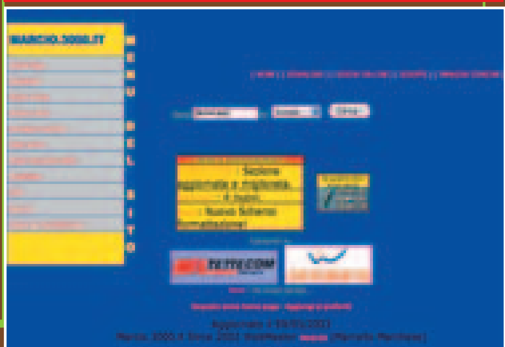
anh.interfree.it



www.devilz.it



www.killmeinthenet.3000.it



www.MARCIO.3000.it

HACKER JOURNAL

STAMPA LIBERA NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

mailto:
redazione@hackerjournal.it

CONDIVIDERE LA CONNESSIONE

Vi prego aiutatemi! Ho un modem alice adsl (il telindus per la precisione) collegato a un Pentium 3 da tavolo ma ho anche un portatile; volevo sapere come fare x collegarmi con l'adsl e con lo stesso modem anche sul portatile. È possibile vero? Siete i più grandi.

Certo che è possibile, e basta installare un router software sul computer che è collegato a Internet, e collegare i due PC in rete (anche solo con due schede di rete e un cavo Ethernet incrociato).
Se hai almeno Windows 98 SE sul computer da tavolo, nel CD di sistema trovi il programma di installazione di Condivisione Connessione Internet (se fai una ricerca nell'help di Windows, trovi tutte le informazioni necessarie).

COMPUTER RUBATI

Mi hanno rubato tra le altre cose anche il mio portatile. Dove il SO era win2000 e w98, anche se stavo installando Linux. La domanda è: riesco a sapere se si collegano con il mio PC e le mie password a internet? E se la risposta è si, come? Aiutatemi: mi hanno rubato circa 3 anni di lavoro, oltre alla mia passione per il PC ed il valore dello stesso… che stronzi figli di…

ronny

Hai tutta la nostra solidarietà. Innanzi tutto, dovresti sporgere denuncia alle forze dell'ordine, e comunicare la cosa al tuo provider (meglio per raccomandata e allegando la denuncia). Il rischio infatti è che i ladri possano compiere reati su Internet utilizzando il tuo account, facendo ricadere la colpa su di te (in realtà, si può benissimo dimostrare che la chiamata non proveniva da casa tua, ma vallo a spiegare a un pubblico ministero che non sa nulla di queste cose…).
Tecnicamente parlando, il provider potrebbe verificare se è stata fatta una connessione usando il tuo account, e dirti da quale numero di telefono è partita la chiamata. In questo modo, è possibile quindi individuare i ladri (o la persona a cui hanno probabilmente rivenduto il computer). Dubito però fortemente che un provider sia disponibile a soddisfare questa tua richiesta; magari se suggerisci la cosa alla Polizia, loro possono fare pressioni più efficaci in questo senso.
Ci sono poi dei programmi che, installati sul portatile, inviano a un indirizzo prefissato ogni indicazione utile alla loro localizzazione, lavorando in modo silenzioso e nascosto. In pratica, il computer rubato "chiama a casa" e comunica la sua posizione. Ne trovi un po' descritti su www.stolenlaptop.com. Occhio però: alcuni potrebbero non funzionare fuori dagli Stati Uniti. Ovviamente però, il programma avrebbe dovuto essere installato prima del furto.

JUKEBOX DIGITALI

Ciao io noleggio videogiochi nei bar e sono appassionato



di informatica. Mi e' venuto in mente di creare un juke box da mettere nei locali. Ora io acquisto i cd per i juke box tradizionali da una ditta che vende dischi di questo tipo.
Se io li copio sull'hard disk sia come wav o mp3 come copia di backup e lascio all'interno del juke box il supporto originale non e' che commetto qualche reato? nota che io farei funzionare la copia di backup.

Patrizio M.

La legge è appena cambiata (ne parliamo nell'editoriale e nell'articolo di pagina 14 di questo numero), e in effetti contempla la possibilità di effettuare copie del materiale protetto da utilizzare in apparecchiature tecniche. Leggendo tra le righe, sembra di capire che tutto sia pensato per agevolare l'uso delle regie automatiche delle radio, che ormai sono tutte basate sull'utilizzo di copie su HD dei brani da trasmettere.
La legge però precisa che deve essere realizzato un accordo tra l'utilizzatore o i suoi rappresentanti di categoria, e i proprietari del copyright. Temo però che la legge sia così fresca che questi accordi non siano ancora stati realizzati. Ti suggerisco di informarti bene presso le associazioni di categoria, oppure rivolgendoti a un avvocato per sottoporgli la questione.

AUGURONI!

Complimenti per essere arrivati fin qui… 1 anno di vita!!!E poi complimenti anche per non aver perso lo spirito che avevate nelle prime uscite (cosa che gli altri periodici non hanno fatto)… un saluto e continuate così'

LordHack

Grazie !!!

MITTENTE REALE DEI MESSAGGI

Salve, volevo sapere se e come è possibile risalire al mittente (nome e cognome reali) di una e-mail del tipo xyzxyz@tin.it.

Lucky

Sì, ma non è alla portata di tutti. Per farlo (sempre che il tizio non abbia nascosto molto bene le sue tracce), bisogna consultare il file di log dei provider che offrono il servizio di mail e di connettività (potrebbero anche essere la stessa azienda). Questo lo possono fare solo le forze dell'Ordine, con un mandato di un magistrato.
In alternativa, potresti provare a fa-

www.hackerjournal.it

re un giochetto sporco: creati un'e-mail anonima tu stesso, e poi mandagli un messaggio dicendogli che ha vinto qualche premio, oppure invitalo su un sito in cui gli chiederai di compilare un modulo coi suoi dati. Se è un pollo, ci casca.

I TESCHI DI CAPITAN HARLOCK?

In risposta al dubbioso sui teschi del n.24 di HJ… Cosa cosa? Come come? Perché ci si lamenta per le copertine Skull-toree di HJ?! Ma che cavolo! Il Jolly Roger è il simbolo di



libertà dei pirati/bucanieri, da sempre in "pericolo" e legati al rischio del loro stile di vita… Vita che poi poteva essre brevissima, tant'e' che spesso il Jolly Roger era accompagnato da Clessidre che ricordavano la sua caducità e l'inesorabile trascorrere del tempo. Perché da così fastidio sulle copertine di HJ che della cultura libera Hacker e' strenua promotrice?
Prendete esempio da Capitan HArloCK (HACK?, mah) simbolo di libertà lealtà e amicizia… (Scusate ma nello scrivere queste righe, un po' me la rido).
Personalmente, sono di parte perche' il mio scooter, come il mio casco e la mia sedia in casa sono marchiati col teschio? Ho pure due belle flag… only
by Jolly Roger…
Per me il Jolly Roger e' un simbolo che vuol dire indipendenza e liberta' (ancora!) e pure se rappresentato da un teschio testimonia per quanto detto caratteri fondamentali (non sempre garantiti) della vita.
Poi siccome non ha le labbra… un teschio sorride sempre!

DarkLink

KAZAA INVASIVO

Salve redazione, volevo fare un po' di veloci chiarimenti. Sono un amante del p2p e ho appena installato kazaa.
Fin qui tutto bene, ma programma in questione è decisamente invasivo.
Premetto che io ho la versione 6.0 di Ad-Aware. Faccio uno scanning e per almeno 50 scansioni compare sempre un certo Cydoor e me lo da come data miner. Continuo a cancellarlo ma riappare sempre (2 reg. key e 1 file). Decido di cercarlo nei meandri del computer e cancellarlo. Lo cancello e quando riapro il computer cosa succede? Kazaa mi da l'errore che ho disinstallato un file di fondamentale importanza e che devo riinstallare tutto il programma…
Kazza non può vivere senza i famosi biscottini ???

Michele

Sì, Kazaa è decisamente antipatico e impiccione. Ne esiste una versione Lite, che dovrebbe essere un po' più pulita. In alternativa, puoi provare i programmi di cui parliamo a pagina 20, alcuni dei quali sono decisamente più rispettosi.

MOLESTIE VIA SMS

Vi pregherei gentilmente di indicarmi se esistono siti o programmi che possano aiutarmi a risalire alla localizzazione (anche solo parziale, meglio se totale), noto l'IP di un computer collegato. Trattasi di un maleducato che importuna una mia collega con frasi oscene, mandando sms tramite www.enel.it. Ho quindi a disposizione l'IP (che ENEL invia) del mittente.

Ing. Massimo A.

***Sì, per esempio puoi usare il comando tracert su Windows (da Start/Esegui inserisci tracert _indirizzo_ip_). Però, se il maleducato ha coperto le sue tracce, rischi di arrivare a un proxy o a un utente ignaro di tutto.
In questo caso, puoi provare a segnalare la cosa a Enel.it o - nei casi più gravi - rivolgerti all'Autorità Giudiziaria, l'unica che abbia il potere di recuperare l'informazione completa del mittente dei messaggi. Anche dopo aver trovato il suo indirizzo IP, infatti, non potresti comunque risalire all'identità della persona, se questa si collega da casa con un modem. Le forze dell'Ordine invece possono richiedere questo dato al provider. Se decidi di fare questa scelta, tieni presente che la conseguenza potrebbe essere un processo.***

UNA PRECISAZIONE

**Vorrei segnalarVi un'imprecisione contenuta in un Vostro articolo: "UUFMDR:
USATE UN FOTTUTO MOTORE DI RICERCA!". L'imprecisione che ho notato verte sull'utilizzo della clausola "OR" per le ricerche su Internet:
<A volte, si possono realizzare ricerche molto complesse aggiungendo delle
parentesi per racchiudere gli operatori logici. Per esempio, con un'espressione di questo tipo:**

(pippo OR pluto) AND topolino

**si trovano le pagine che contengono le parole pippo e topolino oppure pluto
e topolino.>**

In effetti, questo tipo di ricerca otterrà come risultato non solo le pagine contenenti le parole "pippo e topolino" e "pluto e topolino", come da voi riportato, ma anche quelle che contengono tutti e tre i termini (pippo, pluto e topolino). Il vostro esempio è basato, erroneamente, sulla clausola XOR.

Korn

NEWS

HOT!

UNA BRECCIA IN KERIO

È un errorino da poco eppure c'è e permette di bypassare da remoto il firewall Kerio. Il ruleset implementato di default nel firewall accetta qualunque pacchetto UDP in entrata sulla porta 53, rendendo possibile un port scanning mirato a servizi UDP in ascolto. A quel punto contattarli attraverso la porta stessa è cosa praticamente fatta. Per eliminare l'inconveniente basta riformulare la regola specifica per la porta UDP, in modo che accetti solo risposte DNS originate da name server che rispondono ad una query DNS dal sistema client. Panico per tutti gli utenti di Kerio? No per fortuna, visto che la versione buggata pare essere la 2.1.4. Anche se una controllatina alle altre versioni, per scrupolo, noi la daremmo lo stesso…

AL TOPO APPLE SALTERANNO LE ROTELLE?



Sono giunte voci che recentissimamente, solo il 24 aprile scorso, all'ufficio brevetti americano Apple ha depositato la richiesta per un nuovo marchingegno che dovrebbe sostituire la rotellina sul mouse per lo scroll delle pagine. Al posto della rotella dovrebbe esserci un dispositivo a disco che permette di scorrere il documento verticalmente, orizzontalmente e in qualunque direzione ci torni comoda. Insomma una roba troppo avanti. Ciò che non è detto è che al deposito del brevetto segua un uscita del prodotto sul mercato. I Mac Users dunque incrocino le dita del mouse.

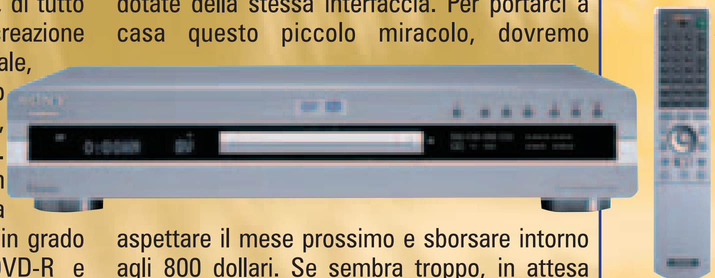
IL MIO COMPUTER HA IL VIRUS DELLA SARS



Non è l'esagerazione dell'invasato di turno che ormai considera il computer alla stregua di un essere umano. Il PC può beccarsi il virus eccome. Da qualche tempo infatti si aggira per la Rete un worm che si propaga via posta elettronica sfruttando la paura della SARS, quella brutta influenzona mortale che sta inginocchiando l'Oriente. Il nome "scientifico" del virus è W32/Coronex-A e viene trasmesso a tutti i contatti presenti nella rubrica del PC infetto. Per restarne immuni non occorrono mascherine o controlli più serrati in aeroporto: basta cestinare mail e relativo allegato che dovrebbero contenere importanti informazioni sulla polmonite atipica. Diverse sono le subject con cui la mail dell'untore si presenta. Tra le più diffuse: "Severe Acute Respiratory Syndrome", "Sars Virus", "Corona Virus", "I need your help" e "deaths virus". Oltre a modificare il registro di Windows, il worm cambierà anche la pagina principale di Internet Explorer, in modo che il browser si colleghi al sito World Health Organization sulla pagina dedicata alla SARS.

NON C'È PIÙ GUSTO

Abbiamo passato notti insonni costateci chili di occhiaie per trovare info, sgami, di tutto e di più sulla duplicazione, ehm sulla creazione di copie di sicurezza, dei DVD? Male, tempo perso che avremmo fatto meglio a impiegare in maniera più produttiva, ci verrà da dire leggendo quanto segue. Sony infatti ha appena annunciato un masterizzatore di DVD multiformato da "salotto". Si chiama RDR-GX7 e sarà in grado di supportare formati DVD-RW, DVD-R e DVD+RW. Come se non bastasse potrà leggere e scrivere CD-R e CD-RW e, oltre alle tradizionali uscite audio/video, è dotato di una porta iLink che consentirà di trasferire file ad alta velocità fra il drive e videocamere digitali dotate della stessa interfaccia. Per portarci a casa questo piccolo miracolo, dovremo



aspettare il mese prossimo e sborsare intorno agli 800 dollari. Se sembra troppo, in attesa che inevitabilmente i prezzi si abbassino, continuiamo con il vecchio sistema di... copie di sicurezza. Almeno le notti in bianco saranno servite a qualcosa.

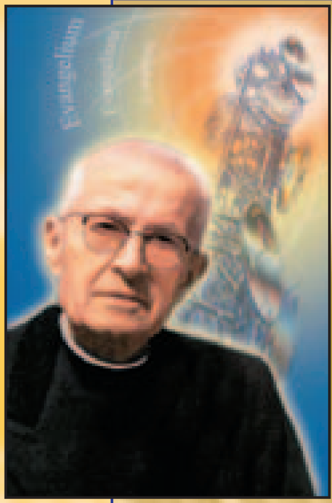
BLOCCARE LE INTRUSIONI? SI CAMBIA METODO



Presto il sistema per rilevare le intrusioni denominato come Statistical o Behaviour Based potrebbe scalzare i più diffusi Signature Based. Il problema più grosso di questi sistemi tradizionali, basati su un sistema di firme e regole, è la velocità di compilazione delle firme stesse, senza le quali il sistema si dimostra cieco. Per includere nella lista un attacco, infatti bisogna individuarlo, registrarlo e analizzarlo. Poi occorre creare la regola all'interno delle firme e distribuire le firme stesse.

Gli Statistical Based Intrusion Detection, SBID, invece hanno tutta un'altra filosofia. In poche parole, una volta determinata la normale attività del sistema, tutto ciò che esce dai parametri della norma viene considerato attività sospetta. Gli SBID analizzano continuamente il normale traffico della rete in cui sono implementati, con una precisione direttamente proporzionale al periodo di attività dell'IDS stesso. Per questa ragione non servono aggiornamenti continui delle firme di identificazione e rispetto ai sistemi tradizionali garantiscono maggiore copertura alle nuove tipologie di attacco.

SAN WEB, SALVACI DAI LAMER



Chi bazzica gli ambienti religiosi o semplicemente è attento alle tradizioni popolari sa bene che in qualunque situazione ci si trovi, c'è sempre un santo a cui votarsi. Esiste il protettore di tutto e di tutti: degli innamorati, dei bevitori, persino dei cornuti. Volevamo lasciare i navigatori di Internet senza patrono? Non sia mai. Il sito http://www.santiebeati.it ha recentemente indetto un sondaggio per nominare il Santo Protettore degli Internauti. In lizza diversi candidati importanti, tra cui persino una donna: Santa Chiara. Il ballottaggio finale si è giocato tra San Giovanni Bosco e il beato Giacomo Alberione, che ha avuto la meglio sul primo totalizzando ben 23.677 consensi. Le votazioni, provenienti da navigatori di tutto il mondo, sono state rigorosissime: un computer un voto. Niente favoritsmi. La motivazione che ha portato a scegliere Don Alberione è che ha sempre dimostrato una grande apertura verso i mass media e le nuove tecnologie della comunicazione. Ora che il popolo si è espresso spetterà al Papa di proclamare ufficialmente il beato come "patrono di Internet". L'uomo propone, il Papa dispone.

TI SPACCO LA CASELLA DI POSTA



Non trasmetti la corsa automobilistica che mi manda in sollucchero? E io, invece di spaccarti la faccia, visto che non so neanche dove venire a pescarti, ti bombardo la posta elettronica con cinquecentomila messaggi. Il ragionamento di questo signore dal carattere un po' bizzarro non è minimamente piaciuto né alla Fox Entertainment che ha commesso l'imperdonabile "errore" di trasmettere una partita di baseball invece di una gara automobilistica Nascar, né alla corte che ha giudicato l'accaduto. L'intemperante Michael Melo rischia ora di dover sborsare 36 mila dollari a risarcimento dei giorni di down causati al sito della Fox Entertainment e di scontare un anno di galera. Chissà se l'avvocato difensore riuscirà a convincere la giuria che il suo cliente, all'oggi pentitissimo, non aveva affatto intenzione di far danni. Non è un cattivo ragazzo: è solo un po' impulsivo...



ARRIVANO I FLICKERS



Nuove creature protagoniste di qualche film americano? Macchè, anche se i flickers col cinema centrano, eccome. Si tratta infatti di elementi disturbanti che verranno inseriti nelle pellicole per evitare atti di pirateria. Secondo i promotori dell'iniziativa, per gli spettatori onesti non cambierà nulla: i flickers non dovrebbero essere né percepibili né dannosi per l'occhio umano. Semplicemente rendono inservibili le copie abusive di film riprese nelle sale cinematografiche. Secondo altri osservatori, però, i flickers sono percettibilissimi e molto fastidiosi. L'unica fregatura, o vantaggio, dipende dai punti di vista, è che questo sistema funziona solo con proiettori digitali. La tecnologia che utilizza i flickers non è nuova, ma è stata recentemente migliorata e messa a punto grazie al patrocinio del governo americano.

HOT!

TESINE ONLINE? FINITA LA PACCHIA

Perché sbattersi una cifra a fare ricerche per quei dannatissimi prof, quando su Internet si trova tutto quanto bello e pronto da copiare? Per tante ragioni. Una delle quali è perché è meglio approfittarne finché dura. Presto infatti la pacchia potrebbe finire. Tre università australiane stanno dando vita a un consorzio che sviluppa un software in grado di controllare se i compiti prodotti dagli studenti sono originali o... un po' troppo ispirati da tesine e contributi vari presenti sulla Rete.

TUTTO IL MONDO È PAESE

Un punto su cui Islam e mondo Occidentale si trovano completamente d'accordo? Il considerare un reato la violazione dei diritti d'autore di software e musica. L'Ulemas Council, massimo organo religioso indonesiano, ha giustificato la presa di posizione contro i pirati informatici, ricordando che i comandamenti islamici vietano di dilapidare le ricchezze altrui e che Allah predica il rispetto della proprietà privata e la fratellanza tra le persone.

ANNI 90 SUL PALMARE





Un punto su cui Islam e mondo Occidentale si trovano completamente d'accordo? Il considerare un reato la violazione dei diritti d'autore di software e musica. L'Ulemas Council, massimo organo religioso indonesiano, ha giustificato la presa di posizione contro i pirati informatici, ricordando che i comandamenti islamici vietano di dilapidare le ricchezze altrui e che Allah predica il rispetto della proprietà privata e la fratellanza tra le persone.

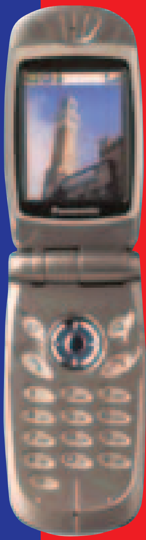
HOT!

IL VESPAIO DI TORVALDS



A Linus Torvalds, padre dell'ormai famoso Linux, è bastato ventilare la possibilità di integrare nel kernel del sistema operativo le tecnologie di digital rights management, per sollevare un polverone mai visto. Si parla, si discute, ci si accapiglia per decidere se è bene o no utilizzare tecnologie di digital rights management, quelle stesse che proteggono il copyright dei contenuti digitali per impedirne l'uso o la copia non autorizzata. Torvalds sostiene che, visto che è impossibile distinguere le firme cattive da quelle buone, la scelta di come usare la firma digitale e le tecnologie di DRM è al di fuori degli obiettivi del kernel e della licenza GPL. Ma che il problema deve essere affrontato. Voi che ne pensate? La discussione è aperta.

FOTO VIETATA, MULTA ASSICURATA



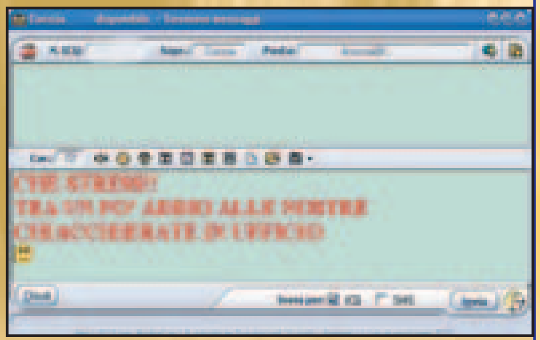
Non facciamoci prendere dai facili entusiasmi suscitati dalle pubblicità dei cellulari dell'ultima ora che ci invitano a scattare foto a destra e a manca come nulla fosse. Se no potrebbe capitarci quanto è successo al povero Gavin Hughes, un gallese che durante un processo ha fotografato con il cellulare il suo amico imputato. Notato da un ispettore che si trovava in aula, lo zelante fotografo è stato immediatamente denunciato e punito con una sanzione di 350 sterline. Leggi locali infatti vietano lo scatto di foto non autorizzate in tali circostanze. Morale: ogni volta che ci prude il dito e ci salta in mente di "cellufotografare" persone sconosciute in luoghi strani… informiamoci sulle leggi vigenti.

NON CI PROVARE PIÙ



Cinque anni di libertà vigilata, rimborso di un bel gruzzolo di dollaroni, nonché riabilitazione psicologica coatta. Ecco cosa si è guadagnato uno studente di Boston che si era lasciato prendere un po' troppo la mano da scorribande informatiche illegali. Cosa ha combinato il signorino? Bazzecole. Ha semplicemente creato un worm che infilatosi nei sistemi protetti della sua università, gli recapitava chili e chili di dati interessanti. Ha intercettato comunicazioni private, si è appropriato di dati personali di altri studenti, infine, giusto per gradire, si è tolto lo sfizio di qualche spesuccia, addebitandola su carte di credito altrui. Come se non bastasse, è persino entrato illegalmente in alcuni edifici del Campus. Vista la pena comminatagli, molti sono convinti che lassù e in tribunale, qualcuno lo ami. Altri giudici, per fatti analoghi di minore entità, hanno prescritto lunghe pene carcerarie.

LAVORA, SCHIAVO!



Quante volte i nostri capi ufficio hanno fatto la voce grossa dicendo: "adesso basta con i programmini succhia tempo e risorse tipo Kazaaa, WinMx, Icq, MSN: qui si lavora, altro che!" Al solito li si lasciava dire: passata la buriana si tornava alle sane vecchie abitudini. Adesso però tira un'aria brutta. IMlogic e SurfControl hanno rilasciato alcuni nuovi tool che consentono anche all'amministratore di sistema più impedito, di filtrare agilmente e selettivamente il traffico da e verso programmi di file sharing e client di messaggistica istantanea. Non serve essere capaci di modificare le impostazioni dei firewall tradizionali, di bloccare tutto il traffico in uscita ed in entrata relativo a client di file-sharing o IM. Per guastare la festa ai dipendenti lavativi bastano pochi clic del mouse. Naturalmente le aziende motiveranno l'adozione di questi sistemi con ragioni di sicurezza aziendale. Eh già… Dannazione, la vita dei lavoratori dipendenti è veramente grama.

TOPPE SALVA WINDOWS



Il caro buon vecchio Bill, Gates naturalmente, si è deciso a regalarci le toppe per riparare i buchi con cui aveva mandato in giro le versioni di Explorer dalla 5.0.1 in poi. Le falle che minacciavano la nostra sicurezza erano ben quattro. La prima riguardava la gestione di alcuni tipi di dialog box; la seconda falla un componente che controlla l'upload di dati; la terza riguardava il modo in cui Explorer interpreta file di terzi. L'ultima falla infine riguardava un buffer overrun contenuto all'interno del componente URLMON.DLL che si occupa di verificare i parametri delle informazioni ricevute da un server Web. Le conseguenze possibili dei bug sono facilmente immaginabili: crackers potevano comodamente avere accesso ai dati contenuti nel disco dei malcapitati utenti. Cioè noi. Le due patch rilasciate, oltre a questi problemi risolvono altri piccoli inconvenienti di sicurezza di Explorer e anche di Outlook. Entrambe possono essere scaricate dal sito Microsoft o attraverso il Windows Update.

➲ CRONACHE DAL WEBB.IT DI PADOVA

Un po' fiera, un po' hack meeting



Webbit è qualcosa di strano nel panorama delle manifestazioni legate all'informatica: una via di mezzo tra la tradizionale esposizione di stand aziendali, e un hack meeting dove gruppi e individui possono collegare i propri computer a una immensa Lan, e condividere esperienze, conoscenze e passioni. Alla sua terza edizione, ha visto moltiplicarsi il numero di community, crew, gruppi di utenti e associazioni, e soprattutto il numero dei seminari gratuiti offerti al pubblico: più di trecento quest'anno. Questo significa che, ogni mezz'ora, era possibile assistere fino a una ventina di seminari diversi.

Più presenti anche le aziende, anche se in una posizione defilata rispetto all'arena delle comunità, vero cuore pulsante della manifestazione. Nelle intenzioni degli organizzatori, Webbit dovrebbe essere una importante occasione per mettere a contatto queste due realtà, superando la barriera che spesso esiste tra di esse: alle aziende si chiede di guardare alla sostanza delle conoscenze e delle tecnologie presentate, senza badare se il relatore ha i capelli di Bob Marley e un pinguino tatuato sul braccio; agli evangelisti dell'open source, si chiede di essere disponibili a lasciarsi contaminare dal "business". Questo più o meno ci ha detto Pier Antonio Maccola, responsabile organizzativo: *«Molto spesso, nel mondo open source ci si ritrova spesso a "parlarsi addosso". Si incontrano persone che già conoscono e condividono la filosofia del software libero, e tutti si ritrovano d'accordo come quando si sono incontrati. Quello che invece cerchiamo di fare con Webbit è mettere insieme due mondi diversi, affinché l'uno possa trarre i maggiori vantaggi possibili dall'altro».*



Di sicuro Webbit è un'occasione unica per piccole comunità o gruppi di utenti: organizzare un raduno o un evento, sarebbe per loro un lavoro molto faticoso (trovare un luogo, organizzare il soggiorno, pubblicizzare la manifestazione). E probabilmente i risultati non sarebbero eclatanti. Qui invece possono incontrarsi godendo del massimo supporto (postazioni per computer, connettività, un'area attrezzata di ogni servizio, e una camerata con brandine per la notte), ed essere sicure di poter parlare a migliaia di persone.

CURIOSITHACK AL WEBB.IT

Prendi quattro XBox chippate, caricaci Linux e le librerie per il calcolo parallelo MIPCH, e otterrai un cluster Beowulf in grado di macinare dati come pochi computer, a un costo molto basso. Questa l'idea dietro a XBoxDebian.org, un gruppo di amici che a Webbit ha dimostrato di saperla lunga.

Come mettere insieme la passione per la meccanica, per l'informatica e per il Subbuteo? Semplice, creando una squadra per la RoboCup, competizione calcistica riservata a piccoli robot! Tutto su www.robocup.org



Un calcolatore vecchio di 30 anni riprende vita, insieme a molti altri computer degli ultimi decenni. Tutto allo stand del Museo didattico di Storia dell'Informatica di Padova, unico al mondo riconosciuto dall'Unesco.
Per info:
www.fwtunesco.org/musi

La Blog Age È COMINCIATA!

A sancirne l'inizio forse gli spaventosi eventi bellici in Iraq, forse il primo convegno italiano di blogger. Nel mirino intanto ancora il ruolo dei media, della rete, dell'informazione e della tecnologia.

In questi ultimi tempi, vi sarete di certo accorti, navigando per il web, **dell'infinita quantità di notizie e di articoli dedicati ai blog** e in particolare di alcuni titoli altisonanti come, per citarne qualcuno, quello del Corriere della Sera, "**Iraq, la guerra dei blog invade la Rete**" (www.corriere.it/Primo_Piano/Esteri/2003/03_Marzo/25/blog.shtml) e di Repubblica, "**In Rete si moltiplicano i blog di guerra**" (www.repubblica.it/online/esteri/iraqattaccodieci/blog/blog.html). Sembra che gli spaventosi eventi bellici di queste settimane abbiano insomma contribuito a divulgare questo fenomeno peculiare della rete a cui a Milano, venerdì 11 aprile, è stato addirittura dedicato un convegno presso la Casa della Cultura: "**Blog Age: La riappropriazione della comunicazione**".



I moderni sistemi di publishing per Blog contengono moduli per calendari, e strumenti per riportare notizie pubblicate da altri blog (Syndication).

>> Blogger di tutta Italia...

Si è trattato della **prima blog conference, made in Italy**, durante la quale scrittori, manager, professionisti della comunicazione, studiosi, studenti, giornalisti ma anche persone comuni hanno potuto incontrarsi per la prima volta nel mondo reale, dopo aver tanto discusso in quello virtuale. La formula dell'evento, organizzato da "Quinto Stato" (www.quintostato.it) e "il Manifesto" (www.ilmanifesto.it), ma alimentato da tutta **blogosfera**, è quella della "tavola rotonda", aperta a chiunque. Molti degli invitati erano muniti di portatile e relativa scheda **wi-fi** (la sala è stata cablata per l'occasione), e persino coloro che non potevano essere presenti all'"incontro", hanno potuto partecipare grazie ad un **Blog Age Aggregator** (un blog collettivo, che ha raccolto tutti i post riguardanti lo svolgimento della conferenza. Tutti hanno riflettuto sul fenomeno dei blog "**nell'ampiezza delle sue varianti culturali**", considerato dagli organizzatori e dagli stessi **blogger** come "**lo strumento più adatto a tradurre la nuova cultura mediatica**", come "**l'esito tecnologico di un lungo processo di riappropriazione dei mezzi di comunicazione**" e come "**ulteriore evoluzione della cultura del freeweb**", ma anche e soprattutto come uno **"spunto" per poter affrontare altre tematiche come la libertà d'espressione**, il diritto d'autore, la letteratura rapportata alle nuove tecnologie, la ricerca tecnico-scientifica, la rappresentazione pubblica del sé. Per lo meno, erano queste le intenzioni iniziali...!



Su Blogger si può creare in pochi minuti un proprio Blog, da pubblicare sul proprio sito o su Blogspot.com, servizio di hosting gratuito o a pagamento.

>> Un fenomeno in crescita

Che quello dei weblog fosse destinato a divenire un fenomeno di così grande significato da meritare persino in Italia tanta attenzione, era forse addirittura prevedibile dal momento che ciò di cui stiamo parlando è di un agile strumento editoriale, che permette a qualsiasi utente, nessuno escluso, in un momento in cui "**la New Economy mira a colonizzare e privatizzare le nuove libertà sorte con l'avvento della Network society**" e "il **mercato tenta d'imporre un accesso dall'alto e gerarchizzato ai contenuti della Rete**", di gestire la pubblicazione dei propri contenuti sul web. Vediamo in che modo! Weblog, lo dice la parola stessa, è un "diario on line".

Diario perché, dal punto di vista tecnico, è caratterizzato dall'aggiornamento quotidiano e dalla sequenzialità rigidamente cronologica dei contenuti (**to log** del resto vuol dire anche "registrare cronologicamente"). È però anche una sorta di giornale o se vogliamo un giornale vero e proprio, in quanto proponendo una rete fittissima di links ad altri blogs, fa sì che si possa passare rapidamente da una visita all'altra, **"in una sorta di filtraggio open source delle notizie presenti in rete ad opera di autori più o meno caratterizzati dagli stessi interessi**" (www.bloggers.it/main/faq.cfm?idFaq=1) e perché non di rado contiene una vera e propria rassegna stampa dei fatti del giorno, come nel caso dei vari blog sorti durante la guerra in Iraq. Grazie al blog, quindi, è possibile pubblicare una notizia — anche quella poco diffusa o celata dagli organi di stampa istituzionali - e allo stesso tempo esprimere pensieri e opinioni a riguardo (vi è persino spazio per i messaggi dei lettori), senza essere obbligati ad autocensurarsi (e di auto censura, i giornalisti professionisti ne sanno più di qualcosa!).



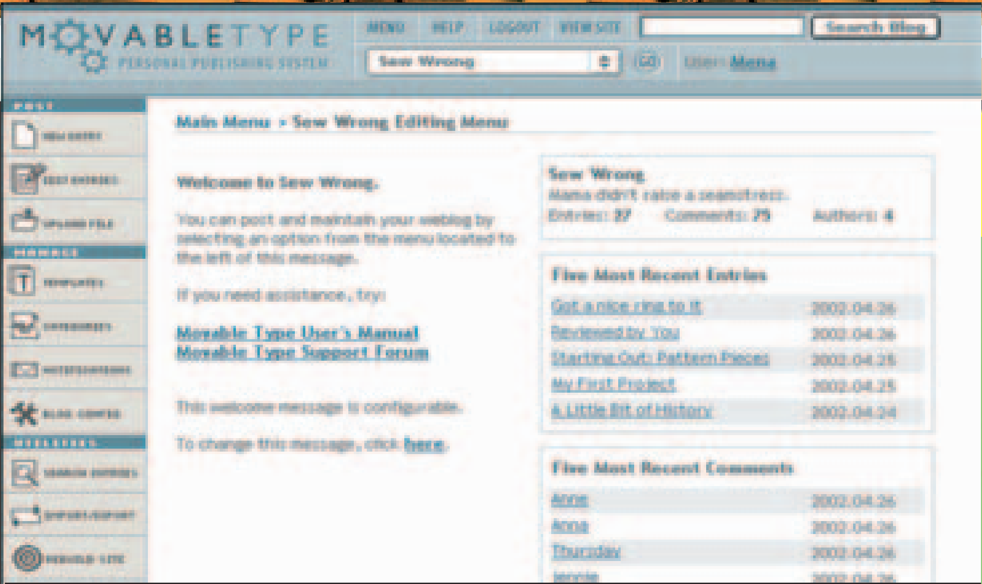


Splinder.it e Clarence.com sono due degli spazi italiani dove si può aprire gratuitamente il proprio Blog.

>> Tra cazzeggio e realtà

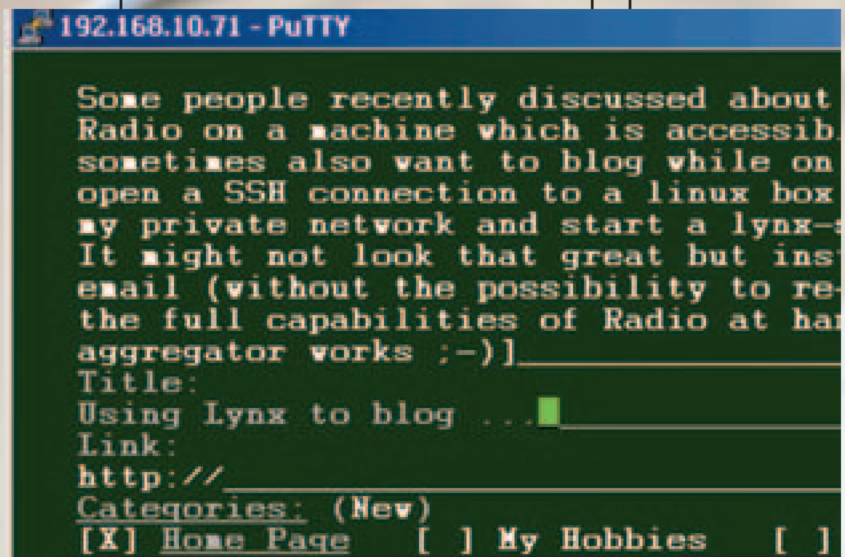
E' possibile che il blog, anche quando sia "cazzeggio", chissà, possa in qualche modo rivelarci alcune realtà, anche spiacevoli, di cui è sempre meglio prendere coscienza piuttosto che far finta di niente! Un libro aperto, insomma, che ci dice chi siamo veramente, come la pensiamo, di che pasta siamo fatti. Il blog, infatti, ed è questo ciò che conta, è soprattutto "cultura" e "informazione", sia quando propende all'individualismo, al diarismo autobiografico, alla rappresentazione pubblica del sé - in genere quando è così è firmato da un solo autore (il weblog di Salam è tutto sommato di questo tipo e ciononostante ha prodotto informazione) -, tanto più quando è di tipo comunitario, impegnato sul piano politico ed etico, teso verso la controinformazione e la lotta verso i media dominanti o la diffusione di contenuti culturali, tecnologici e artistici (www.quintostato.it/archives/000238.html).

Benché alcuni dei partecipanti al **Blog Age** si siano soffermati, in tono polemico, sui limiti delle discussioni emerse durante l'incontro e sulle infinite domande rimaste senza risposta, tutti sembrano d'accordo su di un fatto, almeno credo, e che cioè ci troviamo di fronte ad un potente



Movable Type è un software che permette a chiunque di aprire un blog con ogni funzionalità sul proprio sito, ed è anche il motore che gira sotto a molti siti che offrono un servizio di Blog gratuito.

strumento di espressione, comunicazione e diffusione d'informazione sul quale forse è necessario riflettere ancora. Uno strumento variamente definito soprattutto in toni positivi - per quelli di Quinto Stato è "**un nuovo mezzo di espressione, inquieto,**



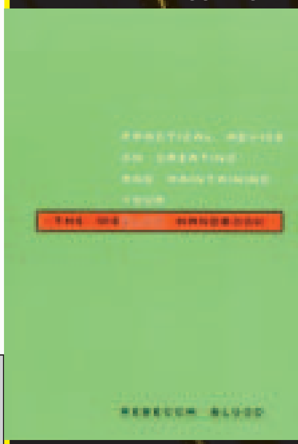
Per pubblicare un Blog si può usare anche un browser testuale, come Lynx, o persino il proprio telefono (www.audioblogger.com).

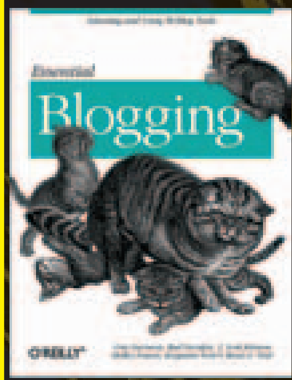
effervescente e ribelle e attraversato dai flussi di scambio delle conoscenze, degli interessi e delle passioni"; per Wall Street Journal "**un medium che riflette il meglio di internet ...informale, anarchico, commercialmente ingenuo ed affascinante**" -, perché "**rompe la dittatura silenziosa della produzione culturale in Italia**" (afferma G. Genna di Carmilla - www.carmillaonline.com), "**mostra l'altra verità**" (dichiara Roberto Vignoli di **Information Guerrilla** riferendosi agli scontri del G8 a Genova www.informationguerrilla.org), perché grazie ad esso "**si è veramente liberi**" (secondo Roberto D'Agostino e Claudio Sabelli Fioretti) e in quanto comunicazione globale, "**permette lo stesso punto di partenza a tutti, dai grandi giornalisti agli ultimi diaristi**" (così afferma lo scrittore Tommaso Labranca (www.labranca.co), e infine perché può far sì che diventi realtà l'esortazione del manifesto di **Indymedia** (www.indymedia.org), l'"Independent Media Center", con cui Carlo Formenti conclude il suo intervento: "**Non odiare i media, diventa tu i media**".

DaMe`
dame@dvara.net

UN PO' DI STORIA

I blog, sebbene un po' diversi nella forma da quelli di cui oggi registriamo questo improvviso aumento, esistono sin dal 1997, anno in cui Jorn Barger, editor del robot wisdom weblog (www.robotwisdom.com) coniò il termine "weblog" (si pronuncia wee-blog, come suggerisce Peter Merholz nel '99) e in seguito inevitabilmente contratto in blog. Posseduti, a quei tempi, solo da coloro che avessero un minimo di conoscenza di html, consistevano per lo più in una serie di link che puntavano a pagine contenenti a loro volta altri link, a pensieri personali, a saggi, ad angoli poco conosciuti della rete o a notizie degne di nota. Questi link erano sempre accompagnati da un commento dell'editore, piuttosto breve, talvolta dal tono irriverente o sarcastico. Nel '98 vi erano già numerosi siti di questo genere. Tra le prime liste di link, ricordiamo la prima page of only weblog (www.jjg.net/portal/tpoowl.html) compilata in quello stesso anno da Jesse James Garrett, editor di Infosit, e quella, dell'anno successivo, di Brigitte Eaton cui si deve addirittura un portale (http://portal.eatonweb.com). Sempre nel '99, si assiste anche ad una rapida crescita di questa forma di scrittura per il web e alla diffusione dei primi tool, rigorosamente free, per pubblicare da sé facilmente e velocemente i propri weblog.





Il primo build-your-own-weblog fu lanciato da Pitas (www.pitas.com); fu poi la volta di **Blogger** (www.blogger.com) realizzato da Pyra e di Edit This Page di Dave Winer (www.editthispage.com).
Per saperne di più sulla storia e l'evoluzione dei blog basta leggere Weblogs: a history and a perspective (www.rebeccablood.net/essays/weblog_history.html), un saggio di Rebecca Blood, autrice per altro di The Weblog Handbook: Practical Advice on Creating and Maintaining Your Blog.

GLI APPASSIONATI DEL RETROCOMPUTING SI INCONTRANO A VARESE



Gusto retrò

Il primo computer non si scorda mai. Per questo, gli amanti dei computer antiquati sono animati da una sfrenata passione.

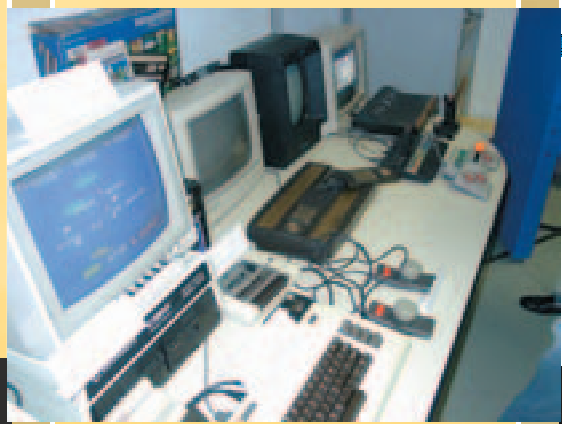
Come anticipato due numeri fa, il 27 aprile, presso il MUel-Museo Elettronico di Varese, ha avuto luogo la prima edizione di "Varese Retrocomputing".
La manifestazione si è articolata su un intero pomeriggio con interventi di esperti e collezionisti di retrocomputing, che hanno parlato e presentato, anche in funzione, numerosi computer che hanno fatto la storia dell'informatica.
Ne parliamo con Bruno Grampa, organizzatore della manifestazione.

Hacker Journal: Come è nata la manifestazione e quali sono i suoi obiettivi?

Bruno Grampa: Varese Retrocomputing è nata con l'obiettivo di affrontare il retrocomputing con un'ottica un po' diversa: non solo recuperare e riparare vecchi computer ma renderli i protagonisti di chiacchierate che ci consentano di imparare qualcosa dalla loro storia. Tutto questo attraverso delle mini conferenze dove poter ascoltare direttamente dalla voce dei protagonisti la storia e le caratteristiche di questi affascinanti oggetti.

HJ: Cos'è per te il retrocomputing?

BG: Mi sono avvicinato al retrocomputing per avere il piacere di possedere quei computer che, da giovane, non avevo avuto il piacere di possedere. Ho scoperto di poter condividere questa mia passione con molte altre persone e che potevo imparare da questi vecchi sistemi molto più di quanto non avessi superficialmente immaginato.
Il successo commerciale di alcuni computer non è stato direttamente legato alle capacità tecniche degli stessi; ci sono computer che sono stati veramente innovativi e che sul mercato non si sono distinti ma dai quali ancora oggi si possono cogliere visioni e idee rivoluzionarie. Non si può non tenere presente che le nostre generazioni hanno visto nascere l'informatica attuale, un avvenimento che per la sua evoluzione e rapidità e' stato veramente unico e formidabile e come tale deve essere documentato.



HJ: Un tuo bilancio su Varese Retrocomputing 2003?

BG: Il bilancio è decisamente positivo: non mi aspettavo una partecipazione così numerosa né il successo di critica che ha seguito la manifestazione.
E' stata una avventura fisicamente e psicologicamente faticosa, ma la soddisfazione è stata veramente grandissima.

HJ: La curiosità o l'oggetto esposto che ti ha affascinato di più ?

BG: Mi hanno affascinato moltissimo il Mac del ventesimo anniversario, il Lisa Apple e tutti i cloni russi dello Spectrum Sinclair. E' stato invece molto gentile e simpatico il sig. Mazzocco che ha partecipato alla manifestazione portando direttamente una serie di oggetti (da lui definite anticaglie!) che ci ha poi illustrato. Non mi aspettavo proprio una partecipazione simile!

HJ: E' prevista una edizione 2004 e in caso affermativo cosa possiamo aspettarci?

BG: Sì, mi piacerebbe moltissimo che Varese Retrocomputing diventasse una manifestazione con cadenza annuale.
Da questa prima edizione abbiamo tratto moltissime idee e spunti che speriamo di mettere in pratica l'anno prossimo. Sicuramente proseguiremo sulla strada che ci ha fin qui caratterizzato e portato fortuna, ovvero le conferenze.
Nel frattempo il sito internet della manifestazione (http://retrocomputing.hal.varese.it) verrà nelle prossime settimane ristrutturato per fornire notizie ed anticipazioni sulle prossime iniziative.

dagostino@nezmar.com

DIRITTO DI COPIA!

COPIED

Le protezioni anti copia dei CD audio limitano l'esercizio del diritto a effettuare una copia personale: noi ci mettiamo una toppa, alla nostra maniera.

Qualche mese fa (Febbraio 2003) è stato pubblicato sulla rivista Audio Review (mensile di elettroacustica, musica ed alta fedeltà) un interessante articolo sulla protezione dei CD Audio, sulla loro effettiva utilità al fine della protezione dalla copia, sulla legittimità di un accorgimento di questo tipo.
Ciò che mi ha colpito di più è che una rivista specializzata che va in mano generalmente, non soltanto ad appassionati di hi-fi ma anche ad operatori del settore, avesse **una posizione decisamente contraria alle protezioni anti copia, perché responsabili in alcuni casi di un peggioramento della qualità d'ascolto**, se non addirittura dell'impossibilità dell'ascolto stesso (mi riferisco alle protezioni che impediscono la lettura del cd su computer e come effetto collaterale su alcuni stereo per auto). Secondo l'articolista di Audio Review, il leit-motiv della protezione dei CD è l'intento da parte delle major discografiche di **legare il brano musicale al supporto, rivoluzionando la concezione che sta invece alla base di parecchie legislazioni sul diritto d'autore tra cui la nostra**. Vi faccio un esempio pratico: se acquistate un CD e volete averne una copia da tenere a casa ed una da ascoltare sul lettore CD della vostra auto, non potreste farlo ma dovreste in teoria (mooolto in teoria) acquistare due copie dello stesso CD. Nella nostra legislazione, invece**, la copia per uso personale è un diritto, quindi tutte le protezioni di fatto sono un impedimento all'esercizio di un nostro sacrosanto diritto.**
Ci accingiamo quindi a descrivere le protezioni anti copia per CD Audio dandovi alcune dritte su come effettuare le copie quando è possibile. Questa è una delle rare volte in cui le tecniche descritte possono e devono essere utilizzate per poter esercitare il proprio legittimo diritto alla copia personale.
Le tecniche di protezione sono in linea teorica di due tipi: le **protezioni che modificano il TOC (Table Of Contents)**, in modo da dare al programma di masterizzazione informazioni errate sulla durata dei brani e sul loro punto di inizio o fine; oppure le **protezioni che inseriscono dei microerrori all'interno delle tracce audio** in modo da bloccare la masterizzazione. Questi ultimi sono i principali responsabili della perdita di qualità. Per riuscire a rilevare il tipo di protezione, e quindi per utilizzare le contromisure del caso, potete utilizzare **ClonyXXL** (www.clonyxxl.redir.it). Vediamo adesso nel dettaglio le più importanti protezioni anti copia per cd audio.

>> CDS (Cactus Data Shield 100-200-300)

Il CDS nelle sue tre versioni è stato realizzato dalla israeliana Midbar, rilevata recentemente dalla più potente Macrovision. La versione 100 e 200 del CDS sono stati adottate dalla BMG. La prima consiste nell'**inserimento di dati falsi nella TOC**, la seconda consiste nella realizzazione di un CD ibrido multisessione in cui vi è una parte contenente i veri e propri fi-



La penna è più forte della spada. E delle protezioni anti copia. Alcune possono essere aggirate tracciando, con un pennarello indelebile, un segno sull'inizio della parte dati.

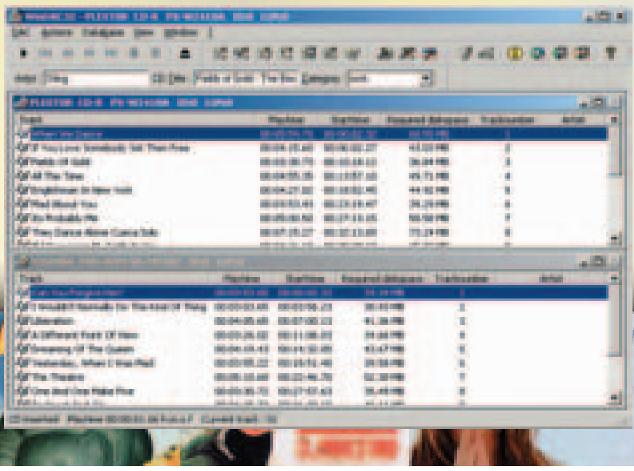


Come succede di solito, per fermare i pirati professionisti, che usano sistemi come questi, vengono colpiti milioni di regolari acquirenti che hanno un solo masterizzatore.

le Audio che sono letti dai normali lettori hi-fi, ed un'altra parte contenente tutti i brani del CD in formato compresso (128 kbps). Quando si inserisce un CD protetto da CDS 200 sul proprio lettore CD-ROM, **viene caricato in automatico un player che legge i brani in formato compresso al posto del lettore di default**. Potete riconoscere questo tipo di protezione oltre che dalla struttura delle sessioni anche dalla presenza dell'eseguibile del player. Un esempio di protezione CDS è il cd di Natalie Imbruglia "While Lilies Island" in cui il player si presenta sotto il nome di CACTUSPJ.EXE. Per copiare i Cd protetti da CDS è necessario prima rippare i brani con un programma di estrazione di file audio come WinDAC per poi ricostruire il CD con un qualunque programma di masterizzazione. L'ultima versione del CDS, la 300, prevede, oltre a tutti gli accorgimenti della versione precedente, anche l'implementazione del DRM (Digital Rights Management) di Microsoft di cui parleremo più dettagliatamente in seguito.

>> Key2Audio

Anche Sony ha sviluppato il suo sistema di protezione chiamato Key2Audio e pure in questo caso il disco è realizzato in multisessione con **divisioni visibili in controluce come nel caso del CDS** Nella prima traccia sono sistemati tutti i brani nel formato standard dopodiché vengono inserite una o più tracce di dati. Questa protezione consiste nell'**inserire degli errori nelle tracce dati che mandano in tilt il lettore CD-ROM** impedendo non soltanto l'acquisizione dei brani su hard disk ma **anche il semplice ascolto su PC**. Uno dei metodi utilizzati per scavalcare questa protezione è l'utilizzo di un nastro adesivo per coprire la traccia dati difettosa. Se infatti guardate il cd in controluce noterete la presenza di una zona vicina al bordo esterno del CD e che ha una riflessione della luce diversa. **Coprite questa zona con una striscia di nastro adesivo e riuscirete ad utilizzare il cd come un normale cd audio** con la possibilità quindi di rippare o semplicemente di ascoltare i brani. Lo stesso risultato può essere ottenuto **anche con un pennarello indelebile**.



Soluzione alternativa a questa tecnica, che possiamo considerare un po' invasiva, è la **masterizzazione utilizzando Clone CD con un buon masterizzatore**. **Le impostazioni da utilizzare in lettura sono:** velocità massima 4x, scanning intelligente dei settori difettosi e lettura dei Sub-channel data sia nelle tracce audio che dati. **In scrittura invece bisogna utilizzare** una velocità massima di 6x, non riparare i Sub-channel data, chiudere sempre l'ultima sessione ed effettuare la calibrazione della potenza del laser. Anche la Sony ha previsto di implementare il DRM di Microsoft nelle prossime versioni del Key2Audio.

>> MediaClòq e SafeAudio

Completiamo la carrellata di protezioni con MediaCloq e SafeAudio, sistemi ormai molto meno diffusi dei precedenti. In particolare il secondo (**SafeAudio**) era stato sviluppato dalla Macrovision in collaborazione con la TTR Technologies finché la Macrovision non ha acquisito la Midbar appropriandosi del CDS, che è diventato l'unico loro prodotto in questo ambito. La protezione consiste nell'**inserimento di errori sulle**

TORVALDS DA IL VIA LIBERA AL DRM SU LINUX!

È di un paio di settimane fa la notizia secondo la quale Linus Torvalds, papà di Linux, avrebbe inviato sulla mailing list degli sviluppatori del kernel del suo sistema operativo un messaggio in cui considerava possibile se non addirittura auspicabile l'implementazione di tecnologie di DRM sul kernel di Linux. Naturalmente un'affermazione di questo tipo ha quantomeno disorientato se non sbalordito la comunità del pinguino, che auspicava uno sviluppo di Linux in direzione opposta. Torvalds dal canto suo ritiene possa essere limitante per linux non implementare tecnologie DRM e che il suo intento è sempre stato quello di creare il miglior sistema operativo possibile e non di fare politica con un software.
Questa affermazione, per quanto legittima ed entro certi limiti condivisibile, crea un divario incolmabile tra due individui che sembravano andare a braccetto fino ad un mese fa ossia lo stesso Linus Torvalds e Richard Stallman, guru del free software. Riuscite ad immaginare un applicativo per linux che funziona soltanto se si scarica la chiave di licenza da internet? Il fatto che papà Linus si sia espresso in questi termini a mio parere non deve stupirci più di tanto se considerate che una delle aziende del progetto Palladium è IBM che ha praticamente adottato Linux pubblicizzandolo gratuitamente come il miglior sistema operativo: ubi maior (IBM), minor (nocopyright) cessat. A questo punto però c'è da chiedersi se l'implementazione di tecnologie DRM sui sistemi operativi Microsoft e la non implementazione degli stessi su linux non sarebbe stata una grossa opportunità di maggior diffusione per il pinguino.
Un'ultima considerazione da fare: vista la sua natura libera e open source, chiunque potrà compilare un kernel Linux senza DRM e distribuirlo liberamente.

tracce audio. Questi errori oltre ad impedire la copia, **impediscono anche il buon ascolto del CD,** poiché spesso vengono interpretati dal lettore dello stereo come fruscii o clip digitali. La copia di backup di un cd protetto da SafeAudio deve essere effettuata attraverso la registrazione dei brani in wav, collegando lo stereo direttamente alla scheda audio. La protezione **MediaCloq** è stata una delle prime introdotte sul mercato e la SunnComm che l'ha sviluppata è stata una delle prime a **subire una denuncia ed a perdere la causa** poiché non c'erano indicazioni sul cd che avvertissero del mancato funzionamento su PC. Inoltre questo sistema prevedeva che l'utente dovesse collegarsi a Internet e riempire un form di dati personali per ascoltare i brani su PC. Se avete un CD protetto con MediaClòq potete fare riferimento al seguente indirizzo per istruzioni dettagliate sulla copia di backup: http://cdprot.cjb.net.



>> Perché tutto ciò?

A questo punto è opportuno spendere due parole sullo scopo per cui queste protezioni sarebbero state realizzate e se hanno centrato l'obiettivo. Possiamo in effetti dire che la pirateria sia sempre esistita: la differenza rispetto a 20 anni fa e che **prima si utilizzavano le audiocassette ed adesso i CD**. Nonostante ciò abbia sicuramente potuto ridurre gli introiti delle major, non penso sia stata l'evento scatenante del ricorso alle protezioni. In realtà quello che non fa dormire la notte i presidenti di BMG, Sony & C. sono sicuramente gli amati mp3, uniti all'utilizzo di un programma di file sharing. Allora la domanda è: **queste protezioni servono ad impedire la diffusione degli mp3? La risposta è No.** Perché? Molto semplice: indipendentemente dalla protezione che possa essere implementata su un cd, **sarà sempre possibile a chiunque effettuare una copia dei brani su PC con un semplice collegamento stereo-scheda audio** e un qualunque programma di registrazione audio. Direte voi: "Questo è vero, ma la qualità?". Il problema qualità non si pone poiché **la qualità della registrazione con le recenti schede audio è comunque superiore all'Mp3** Per cui se convertiamo a 192 kbps un file rippato (ossia una copia digitale perfetta del brano) o una registrazione audio otteniamo quasi lo stesso risultato.

È da questa inefficacia di fondo delle protezioni anti copia che nasce l'esigenza di utilizzare le tecnologie DRM.

>> Digital Rigths Management

Il DRM (Digital Rights Managment) che ho citato in precedenza comprende tutte quelle tecnologie che hanno come scopo la protezione del diritto d'autore attraverso **l'impedimento di attività non autorizzate su qualunque prodotto dell'ingegno umano che si trovi in formato digitale**. Possiamo considerare il DRM come l'antitesi degli standard aperti: l'intenzione è quella di **blindare applicazioni, musica, film e testi attraverso la crittografia**.
Microsoft sta già mettendo in pratica il DRM nelle nuove versioni del Windows Media Player. L'implementazione della casa di Redmond prevede il la cifratura del file del brano che può essere distribuito sia su CD sia via Internet **in modo che sia possibile ascoltarlo soltanto a chi possiede la chiave di licenza del brano stesso**. La licenza in questo modo può essere diversificata creando delle licenze "scalabili", cioè una chiave potrebbe prevedere ad esempio **soltanto l'ascolto sul computer in cui il brano è stato scaricato**, mentre un'altra potrebbe prevedere la **possibilità di copia su un lettore portatile**. Il cuore del nuovo sistema Microsoft è il Windows Media Rights Manager il cui flusso operativo è il seguente:

1 Viene effettuata la cifratura del file multimediale che può essere distribuito all'utente su cd o attraverso Internet;
2 L'utente si collega al servizio License Server del WMRM che si occupa della registrazione ed autenticazione dell'utente e dell'invio della chiave di licenza;
3 L'utente utilizzando la chiave con il suo Windows Media Player decifra e legge il file o lo copia in base ai diritti presenti nella sua licenza.

Per maggiori dettagli sull'architettura del WMRM vi consiglio di consultare il sito Microsoft con il link che trovate nel riquadro in queste pagine.
A differenza di quanto accade con la rimozione delle protezioni anti copia (per le quali è vietata solo la vendita e diffusione di prodotti in grado di superarle, ma non il loro effettivo aggiramento, se è a scopo personale e non a fini di lucro), **l'atto della rimozione o alterazione delle tecnologie di DRM è un reato in sé e per sé.**

Roberto 'decOder' Enea
enea@hackerjournal.it

LINK UTILI

www.macrovision.com/solutions/audio/ Sito della Macrovision attuale proprietaria del sistema CDS
www.windac.de Sito di WinDAC
www.key2audio.com Sito del sistema Key2Audio di Sony
http://www.microsoft.com/windows/windowsmedia/drm.aspx Sito dell'implementazione Microsoft del DRM
http://punto-informatico.it/servizi/ps.asp?i=43896 Torvalds e il DRM



ALLARME VIRUS

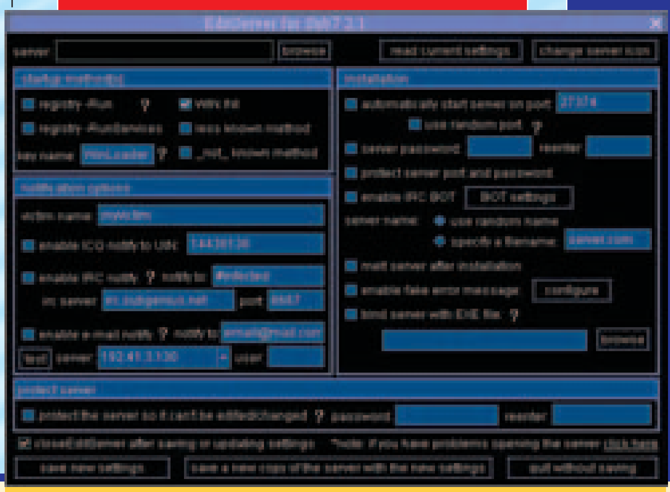
Tranquilli, niente a che vedere con la SARS, ma si tratta ugualmente di qualcosa di molto fastidioso: i virus informatici. Impariamo a conoscerli meglio per combatterli più efficacemente.

Da qualche anno a questa parte stiamo assistendo a una grande evoluzionedelle tecnologie informatiche rivolte alla sicurezza, e in particolare **antivirus e firewall sono diventati strumenti di diffusione di massa**, specialmente con l'utilizzo delle reti geografiche come Internet.
Problemi causati da virus e da altri programmi maligni (in inglese malware) sono oramai sulla bocca di tutti, e talvolta ne parlano (spesso a sproposito), anche telegiornali e trasmissioni televisive.
Qualche anno fa **creare un virus era compito davvero arduo**: bisognava avere conoscenze specifiche di linguaggi di basso livello come l'assembler, inoltre era necessario padroneggiare in dettaglio l'architettura dei sistemi IBM compatibili per poter **controllare la memoria RAM e rimanere residenti in essa** (TSR) con lo scopo di riprodursi su altri file e di infettare l'intero computer.
Molti di questi termini potrebbero avervi messo in difficoltà, specie se siete alle prime armi, ma i concetti da tenere a mente sono molto semplici e procedendo con ordine esamineremo tutte le principali tecniche di attacco virale.

>> Categorie di virus

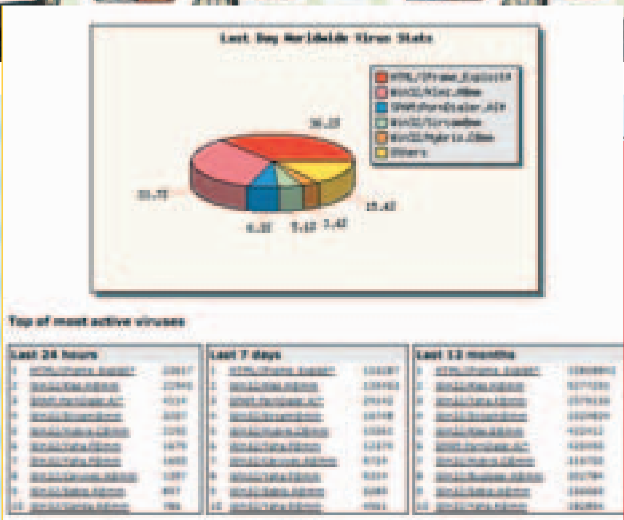
Innanzitutto bisogna **distinguere i virus in numerose categorie**, classificandoli come si farebbe con dei ceppi biologici, al fine di poterne delineare differenze e peculiarità.
Partendo dalle origini, il termine virus è stato coniato qualche decennio fa e quindi oggi molte cose sono cambiate e numerosi malware sono spesso considerati dei virus. In particolare differenti dai virus prima erano considerate le **Bombe logiche**, i **Conigli** ed infine i **Vermi** (oggi molto diffusi).

Per Bomba logica si intende intendiamo un programma **creato allo scopo di arrecare danno attivandosi in determinate condizioni**. Numerose di esse sono state spesso considerate dei virus, e hanno dato alcuni fastidi agli utenti in determinati giorni dell'anno, in opportune ricorrenze scelte dagli autori.
I Conigli (o rabbit) erano chiamati tutti quei programmi che, al giorno d'oggi con moderna terminologia definiremmo **Denial of Service (DoS)**. In pratica il loro intento era quello di **saturare le risorse software di un sistema come tempo della CPU, memoria, rete eccetera**. Ultimamente abbiamo assistito a bug come quello di alcuni controlli ActiveX che per un problema di buffer overflow potevano esaurire le risorse di sistema provocando un crash dell'intera macchina.
Caratteristica comune alle due tipologie presentate è il fatto che entrambi **non possono riprodursi, al contrario invece dei worm il cui scopo principale è essenzialmente questo**.
Il worm ha la capacità di propagarsi in rete e di installarsi su altre macchine, e spesso sfrutta dei **bug conosciuti che gli amministratori di sistema incompetenti o pigri non hanno ancora risolto con delle apposite**



Sebbene i cavalli di Troia non siano dei veri e propri virus, un buon antivirus dovrebbe riuscire a identificarli e renderli innocui.

CIMICI, MICROSPIE E



Rav Antivirus ha una pagina con le statistiche di diffusione dei virus aggiornate in tempo reale. È all'indirizzo http://www.rav.ro/ravmsstats/



Un'altra interessante fonte è l'enciclopedia dei virus di AVP, che trovate su www.avp.ch/avpve/

patch. Talvolta a livello mondiale si è addirittura assistito a vere e proprie **epidemie che nell'arco di poche ore hanno colpito server strategici** e paralizzato il traffico di numerose intranet.

>> Cavalli di Troia e keylogger

Un'altra categoria di riferimento, di cui vorrei parlare in maniera separata è quella dei cavalli di troia (trojan) di cui oggi c'è una vera e propria diffusione massiccia, specie **da parte di tutti coloro che atteggiandosi ad hacker cercano di percorrere la strada più breve per entrare nel computer della loro vittima**.

Trojan qualche anno fa significava programma, che apparentemente aveva funzione di compiere una determinata operazione, mentre in realtà era preposto a minare la sicurezza di un sistema e a creare una breccia per potervi entrare in un qualsiasi momento (stesso significato di **backdoor: accesso dalla porta di servizio**, lasciata aperta dall'autore maligno).

Oggi però le cose sono un po' cambiate, ed infatti le backdoor o trojan stanno sempre più spesso assumendo connotazioni "stealth", mascherandosi agli occhi degli utenti (spesso anche dei più smaliziati) e permettono un pieno controllo della macchina da remoto sia per ciò che riguarda la **visualizzazione dei tasti digitati dalla vittima** (keylogging) sia mediante **l'ascolto delle conversazioni dell'ignaro utente attraverso il microfono di sistema**. Esempi di backdoor ad ampia diffusione sono Back Orifice e Netbus. Il motivo della grande pericolosità di tali programmi è stato quello che gli autori hanno rilasciato pubblicamente i sorgenti delle applicazioni, **permettendo agli utenti, anche poco esperti, di dare origine ad infinite varianti**, sempre più difficilmente rilevabili e costringendo gli utilizzatori di PC, più che a fidarsi degli antivirus, a non aprire alcun file allegato per evitare ogni possibilità di contagio.

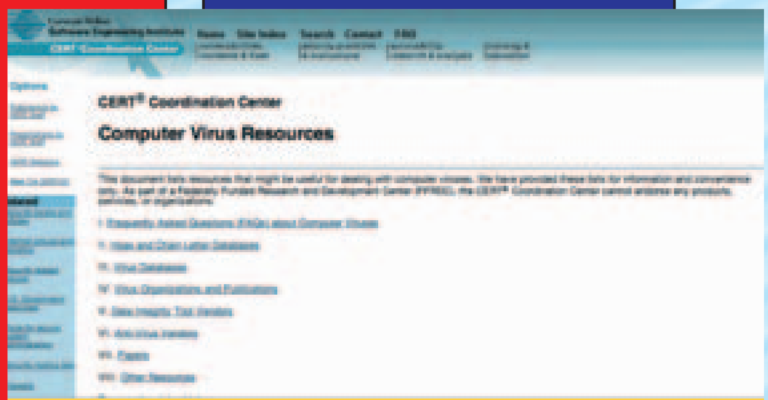
Altri programmi con funzione di trojan sono proprio i già citati **keylogger**, applicazioni utilizzate anche nelle indagini svolte a computer (computer forensic) **in grado di catturare ogni tasto premuto dall'utente e di memorizzare oltre le password ed i nomi utente anche alcune informazioni vitali come le chiavi crittografiche di utilità come PGP**, per poi successivamente decrittare file pressoché impenetrabili. Un sistema commerciale dalle grosse potenzialità è, per esempio, **Amecisco Stealth Keylogger**, capace di installarsi come driver di tastiera, e di avere dunque il massimo della libertà in fatto di intercettazione e di invisibilità!

Tornando comunque ai veri e propri virus, ovvero a quei programmi creati con lo scopo primario di riprodursi per infettare, non abbiamo ancora delineato quali possano essere gli attacchi effettuabili da essi. Dovremmo infatti distinguere i virus veri e propri in altre sotto categorie, come i **virus da boot sector, i virus degli eseguibili, i virus delle macro, ed io aggiungerei gli exploit ed i retro-virus**.

Cominciando con ordine, i virus da boot sector sono stati una delle minacce più pericolose di questi ultimi anni, visto che **attaccando il sistema addirittura nel momento del boot rendevano vano ogni tentativo maldestro di disinfezione**. I virus più diffusi però da sempre, sono quelli dei file eseguibili, che con la loro capacità di infettare i programmi possono portare alla paralisi dell'intero sistema in breve tempo.

>> Tecniche di mascheramento

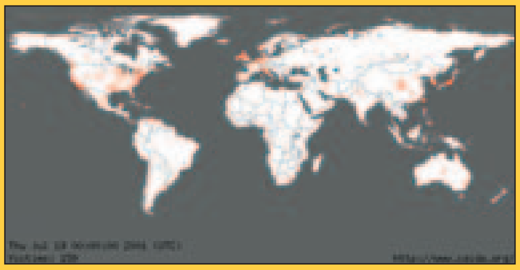
Sicuramente questa è la tipologia più studiata e discussa visto che ritroviamo alcuni "capolavori" in grado di nascondersi all'occhio degli antivirus con svariate tecniche di mascheramento degne di nota. In particolare, per riprodursi, **teoricamente un virus dovrebbe letteralmente appendersi ad un altro eseguibile** per fare in modo che ad ogni avvio dell'applicazione vi sia di conseguenza un'esecuzione di esso stesso. Adottando una strategia di questo genere, però, un qualsiasi antivirus o piccola



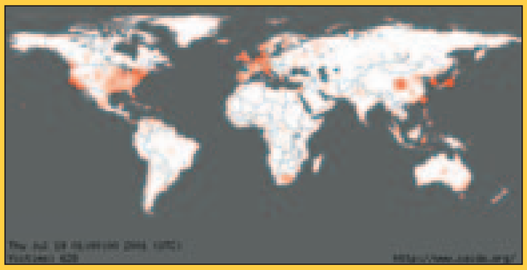
Se cercate informazioni sugli antivirus, queste pagine del Cert sono un buon punto di partenza: ci sono link alla documentazione presente sui siti di vari produtori di antivirus, università ed enti pubblici e privati. Lo trovate su http://www.cert.org/other_sources/viruses.html

EPIDEMIA DI CODE RED

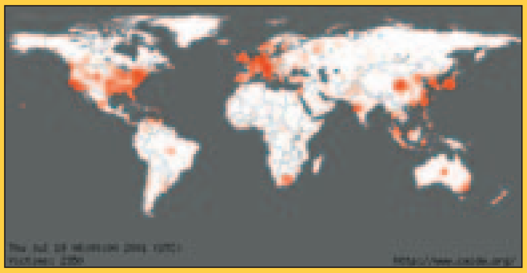
Questa sequenza, tratta dall'animazione disponibile all'indirizzo http://www.caida.org/analysis/security/code-red/, mostra la diffusione del worm Code Red nelle prime 24 ore dalla sua individuazione.



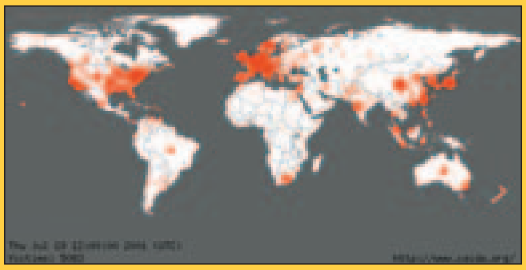
Ora 0
Quando ci si è accorti della sua esistenza, Code Red aveva già contagiato 159 server.



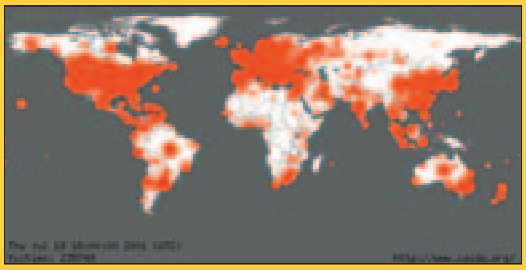
Ora 1
Dopo solo un'ora, le vittime sono diventate 628, sparse sui quattro continenti popolati.



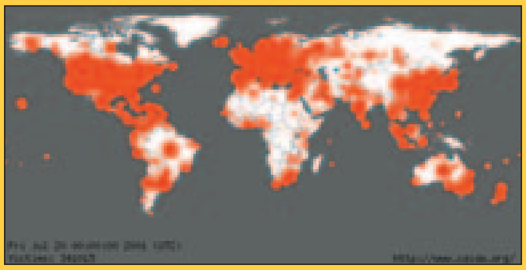
Ora 6
Il contagio cresce: siamo a 2350 vittime, ovviamente concentrate nelle zone di maggiore informatizzazione.



Ora 12
È passata mezza giornata, ma Code Red ha lavorato alacremente, superando i 5.000 server infettati.



Ora 18
In queste ore Code Red fa il suo salto di qualità: anche se è difficile apprezzare la differenza sulla mappa, le vittime passano a più di 235.000



Ora 24
Dopo solo un giorno, il verme si è insediato in quasi 350.000 server in tutto il mondo.

utilità creata per l'occasione si accorgerebbe di un **cambiamento nelle dimensioni di un file** ed ecco allora che la bravura dei programmatori si è sbizzarrita in molte maniere…
Altro fattore trainante, che ha contribuito alla diffusione di virus specificamente progettati per infettare gli eseguibili, è stata l'adozione di **sistemi operativi come Windows che hanno facilitato la programmazione** di aspetti come l'esecuzione in memoria dei programmi e la capacità di restare residenti in memoria con poco sforzo in termini di programmazione.

>> Virus di oggi

Con l'introduzione di nuove ed avanzate funzionalità in applicativi come software di videoscrittura e di foglio elettronico, si è diffuso un tipo di attacco addirittura impensabile qualche anno fa: **i virus delle macro**.
Uno dei più famosi è stato sicuramente "I love you" che tanto ha fatto parlare di sé soprattutto presso la stampa non tecnica, e che ha recato danno ad un ingente numero di postazioni, malgrado le capacità di programmazione di un simile virus siano alla portata di molti.
Il vero problema della proliferazione di tali macro maligne, infatti, è insito proprio nel fatto che **la creazione di un virus di tal genere è un'operazione estremamente semplice**, specie se raffrontata alle altre tipologie virali.
Visual Basic for Application infatti ha costituito e costituisce tuttora un utilissimo/pericolosissimo ambiente per programmatori maliziosi (e non solo) e utenti finali.
E degli Exploit che dire allora? È una tipologia di attacco alla sicurezza di sistema, a mio parere, da trattare al pari dei virus e quindi come ulteriore minaccia alla sicurezza informatica.
Per problemi di buffer overflow, infatti, si è potuto **ingannare il software Outlook** e molti programmatori hanno sfruttato tale debolezza per far eseguire a tale client di posta elettronica gli allegati che contenevano, inutile dirlo, dei virus o alcuni programmi troiani!
Passando in rassegna la categoria dei **retrovirus**, ovvero tutti quei programmi che cercano di rendere vana la protezione antivirus o quantomeno tentano di camuffarsi agli occhi dei vari engine antivirali, c'è da dire che di questo argomento si è già discusso sul numero 22 di HJ con un mio proof-of-concept, sebbene ci sia da precisare che questa tipologia di attacco risale già agli anni del DOS con diverse creazioni.

Paolo Iorio
www.paoloiorio.it

SOTTO CATEGORIE DI VIRUS

Nell'eterna lotta per evitare di farsi identificare dagli antivirus, gli autori di programmi malevoli hanno dato vita a varianti sempre più raffinate dei loro codici. Ecco acuni esempi:

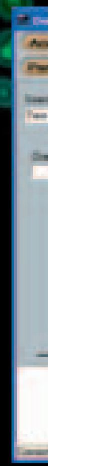
Virus Mutanti
Modificano il proprio codice ogni volta che vengono copiati, in modo da non poter essere facilmente identificati dagli antivirus.
Virus Cifrati
Il codice del virus viene cifrato, in modo da non rendere riconoscibili le istruzioni nocive da parte degli antivirus. Prima dell'esecuzione, il motore crittografico decodifica il tutto e lo esegue.
Virus Multipartiti
Agiscono sia come virus del boot sector, perché entrano in esecuzione all'avvio, ma si diffondono attaccandosi ai file eseguibili.
Virus Polimorfi
Sono un'evoluzione più sofisticata dei virus mutanti.

ALCUNI SOFTWARE E NETWORK P2P MENO CONOSCIUTI

TANTI MODI PER CONDIVIDERE

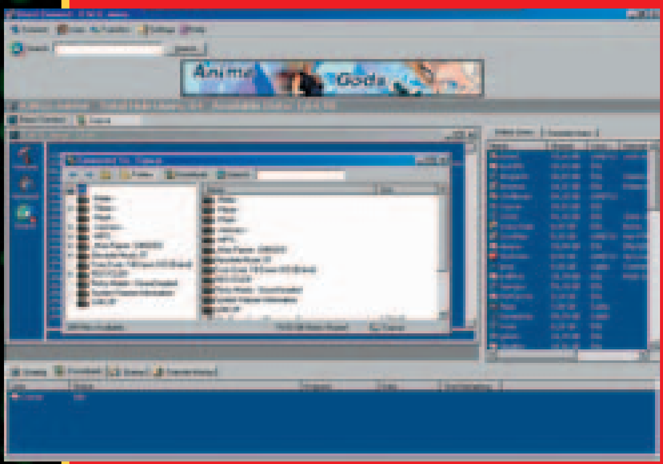
{RoSwEIL}

Sugli scorsi numeri abbiamo esaminato i più blasonati sistemi di file sharing; è tempo di dare spazio anche ai meno conosciuti!



DIRECT CONNECT

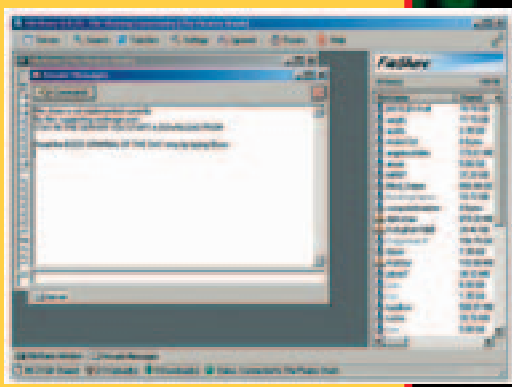
Direct Connect è un programma di file sharing che è rimasto nascosto per tanto tempo ma ora sembra essere uscito allo scoperto e raccoglie sempre più utenti. Per quanto riguarda il network su cui funziona, è piuttosto simile a eDonkey2000 e OperNap. Gli ideatori di Direct Connect hanno lavorato a un software che funga sia da client che da server, e che attualmente viene utilizzato da oltre 40.000 utenti in tutto il mondo. Direct Connect è in grado di effettuare ricerche di file anche molto particolari grazie alle numerose opzioni di ricerca avanzata di cui è fornito. I punti deboli del programma sono però l'interfaccia incasinata, che può creare un pò di confusione, e la difficoltà in alcuni casi di connettersi ai suoi server. Per gli utenti domestici, i punti deboli non finiscono qui: scaricare Direct Connect non è gratis ma bisogna esporre alcuni banner per poter avere l'accesso ai suoi server (cosa che rallenta lo scaricamento e la navigazione con modem). Le funzioni principali di DirectConnect sono raggiungibili dai relativi bottoni situati nella parte alta del programma e sono:



Connect Mostra la finestra per selezionare e connettersi a un server.
Uses Con questa opzioni si può visualizzare o nascondere la finestra degli utenti e serve a mostrare una lista di tutti gli utenti connessi al server su cui ci si trova.
Transfers Mostra i download e gli upload in corso.
Settings Serve a modificare le opzioni per il download e l'upload, per configurare i programma e il network e cambiare la propria identità.
Search Una volta connessi ad un server, si può cercare un file tramite questa opzioni. Ciccando sul globo è possibile effettuare una ricerca avanzata per definire al meglio i parametri di ricerca.
Direct Connect è attualmente fermo alla versione 1.0 rilasciata oltre due anni fa ed è scaricabile dal sito del produttore:
www.neo-modus.com.

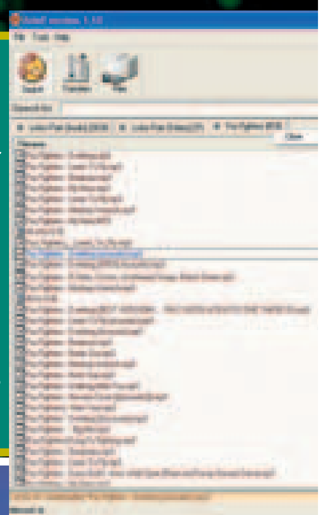
FILESHARE

FileShare è l'ultimo programma di file sharing ad aver attuato fondamentali modifiche per una maggiore sicurezza e protezione da spam, spyware e virus sempre in agguato tra gli innocenti file che si vanno a scaricare. Proprio per questo è sicuramente preferibile ad altri client come KaZaA, eMule, Direct Connect, iMesh che basano proprio i propri guadagni sugli spyware e banner che sfruttano a discapito degli utenti. FileShare è uno dei più "puliti" client nel senso che è non contiene spyware, pubblicità, pop-up e virus. L'ultima versione è la 1.4.2 è permette di visualizzare graficamente i file incompleti e visualizza i server degli utenti connessi da cui si sta scaricando qualche file. Sono stati anche risolti alcuni bug presenti all'avvio dell'applicazione. Il punto debole è che è possibile utilizzare FileShare solamente con Windows; l'ultima versione è scaricabile dal sito
http://bbn.datakill.com.



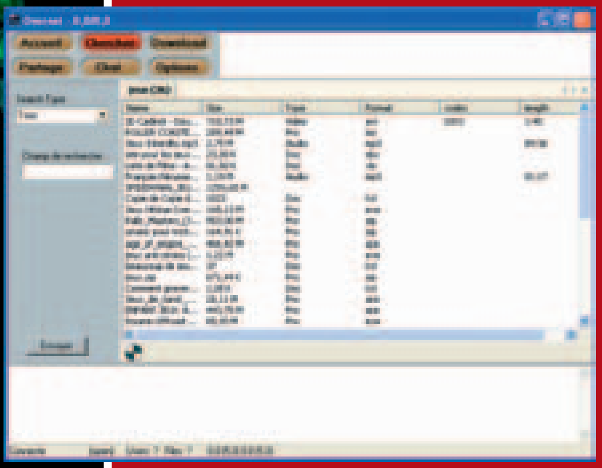
XOLOX

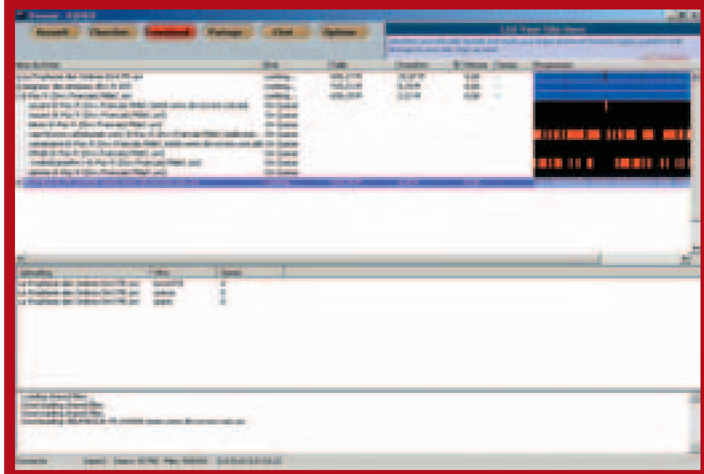
XoloX è uno dei più popolari client in circolazione nel mondo del peer to peer ed è ritornato recentemente alla ribalta con enorme piacere dei migliaia di utenti che lo preferiscono a tutti gli altri. A causa di difficoltà finanziarie e problemi legali XoloX ha un passato piuttosto discontinuo. Comunque una corte di appello tedesca permise nello scorso Novembre l'uso di KaZaA che non com-



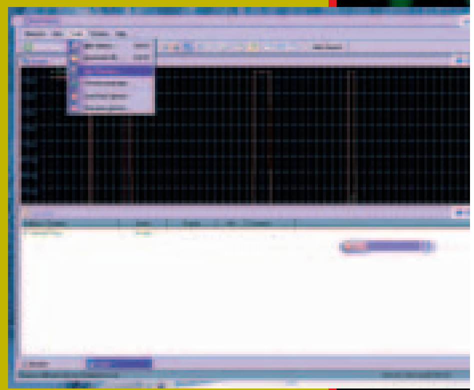
OVERNET

Overnet è senza dubbio uno dei migliori software per il file sharing in circolazione sul web. Caratterizzato da un'interfaccia regolabile con l'uso di skin personalizzati, funziona su dei propri server senza che ce ne sia uno centrale, troppo facile da localizzare e chiudere dalle case produttrici. Le ultime modifiche apportate permettono una ricerca molto più efficiente e download sempre più veloci grazie al protocollo MFTP: è possibile così, come in altri software simili, di scaricare uno stesso file diviso in parti da più utenti, garantendo la sicurezza e l'affidabilità dei file scaricati e aumentando notevolmente la velocità. Altro punto di forza di Overnet è quello della compatibilità con tutte le principali piattaforme e sistemi operativi in circolazione: da Windows a Linux ai Mac (anche se per questi è solo a linea di comando). Con un'interfaccia grafica seguita da uno spazio per i comandi manuali sotto Windows, è forse uno dei programmi peer to peer più affidabili e sicuri. È possibile scaricare l'ultima versione di Overnet dal suo sito ufficiale www.overnet.com.





SHAREAZA



Shareaza è apparso all'improvviso sulla scena peer to peer riscuotendo un discreto successo. Questo particolare software sembra avere più di una personalità: ciccando semplicemente col mouse è possibile trasformare il client a proprio piacimento, da un'interfaccia semplicissima come quella di XoloX ad una molto più complessa e completa come quella di Gnutella; in poche parole è un software adatto a tutti, sia ai principianti che ai più esperti. Tra i punti di forza di Shareaza troviamo la possibilità di effettuare download simultanei senza troppe ricadute sulla connessione, un ottimo motore di ricerca per i file, grande efficienza dei server e, come detto prima, un interfaccia senza paragoni. All'avvio Shareaza si connette automaticamente alla community di Gnutella per ottenere una maggiore disponibilità di materiale scaricabile; importante negli ultimi tempi, è il rispetto per la privacy dell'applicazione che è ripulita da ogni spyware o adware. I comandi principali, disponibili sia nell'interfaccia basilare che in quella più complessa sono i seguenti:

Connect/Disconnect Permette di connettersi e disconnettersi ad uno dei server Gnutella che ospitano gli utenti di Shareaza con un semplice clic del mouse.

Home E' una particolare opzione che permette di navigare i Shareaza molto più facilmente che in altri programmi di file sharing.

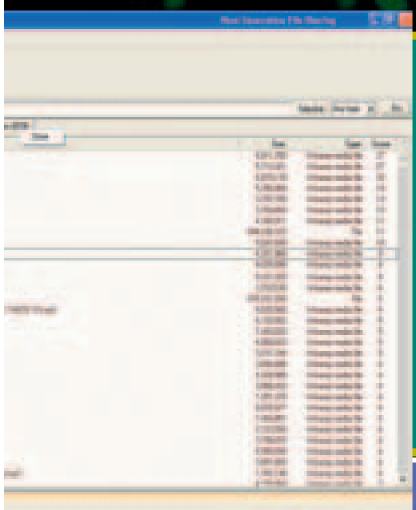
Library - Shareaza è provvisto di un'eccellente organizzazione dei file scaricabili; con questa opzione è possibile tenere sotto controllo al meglio i propri file a disposizione degli utenti.

Network Questa finestra gestisce la propria connessione al server Gnutella.

Transfers Una delle finestre più importanti quella che permette di visualizzare i propri upload e download, con dettagliate informazioni su ogni singolo file e sulla sua provenienza.

Open New Search Già il nome lascia intendere che si tratta della fondamentale opzione per la ricerca dei file.

Shareaza è attualmente arrivato alla versione 1.6 rilasciata quasi un anno fa. E' possibile scaricarla gratuitamente dal sito ufficiale www.shareaza.com.



portava infrazioni nelle leggi sui copyright. Questo episodio incoraggiò gli sviluppatori di XoloX che resuscitarono la propria opera a cui sono state apportate numerose e fondamentali modifiche. La nuova versione rilasciata a Dicembre 2002 include alcuni importanti aggiornamenti come le informazioni sui bitrate, la compatibilità con Gnutella e l'aumento dell'efficienza dei propri network. Ci sono solo quattro sezioni in XoloX, tutte raggiungibile con un semplice clic di mouse:

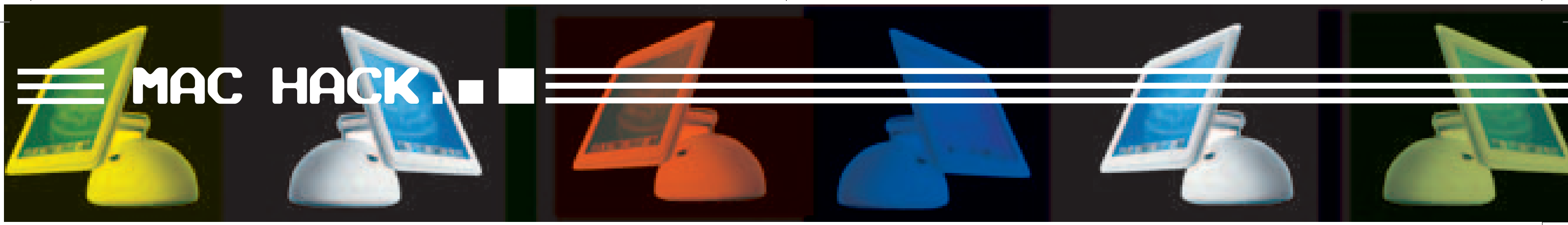
XoloX Da considerare come "l'HomePage" del programma, questa finestra permette di tenersi aggiornati sugli ultimi aggiornamenti di XoloX e sulle sue novità.

Search La fondamentale finestra per la ricerca dei file che si vogliono scaricare.

Transfers Mostra gli upload e i download in corso con la possibilità di modificare le opzioni e i parametri con cui questi vengono effettuati.

Files Mostra tutti i file sul proprio computer scaricati e disponibili agli altri utenti.

L'ultima versione di XoloX è la 1.41 ultra che si può scaricare da www.xolox.nl

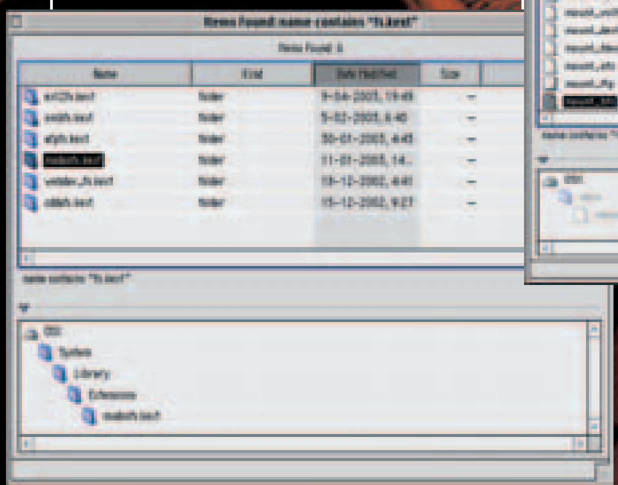


QUALI SONO I FILESYSTEM SUPPORTATI DA MAC OS XA

DisCo mix

HFS, UFS, SMB e gli altri: esploriamo il cosmo variegato dei numerosi filesystem supportati da OSX, con un occhio al passato del Macintosh ed uno al mondo sempre più vicino di Linux e Windows.

Secondo le note tecniche di Apple il filesystem di Darwin/OSX è progettato su **un'architettura "Virtual File System" (VFS) modulare** che rende possibile aggiungere nuovi filesystem e usare e estendere le funzioni di quelli supportati, tra cui HFS, HFS+ (noti anche come "MacOS" e "MacOS esteso"), ISO9660 (quello dei CD-ROM di Windows) ed altri ancora.
L'implementazione di Apple è diversa da quella in altri sistemi BSD: **i vari filesystem sono estensioni del kernel, cartelle speciali con estensione ".kext" simili come concetto ai moduli del kernel in Linux.**



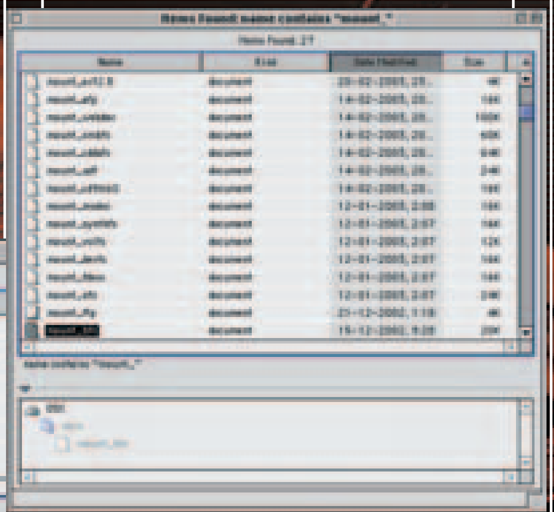
Queste "estensioni" risiedono in "/System/Library//Extensions/" e molte hanno il nome che termina per "fs.kext"

Ad esempio

```
/System/Library//Extensions/msdosfs.kext
```

è il modulo che abilita il file system FAT dell'Ms-Dos, mentre

```
/System/Library//Extensions/udf.kext
```



è quello relativo all'UDF, filesystem usato dai masterizzatori su CD riscrivibili.
Un altro modo per controllare i vari filesystem supportati è quello di **dare una sbirciata a quanto supportato dal comando "mount"** ad esempio da Terminale, prima spostandosi nella cartella nascosta "/sbin" scrivendo

```
cd /sbin
```

e poi facendo un elenco di quanto disponibile con

```
ls | grep mount_
```

Vediamo però dal punto di vista pratico i principali filesystem, le loro proprietà e modalità d'uso.

>> HFS+ contro tutti

I primi due con cui l'utente di OS X fa subito conoscenza sono quelli proposti per l'inizializzazione del disco (la formattazione) al momento dell'installazione del sistema: HFS+ e UFS.
Il primo, detto anche **Hierarchical File System +**, o **"Mac OS Extended"** ("Mac OS Esteso"), è già noto da diversi anni agli utenti dei precedenti sistemi, per la precisione dalla versione 8.1 del Mac OS, dove ha affiancato il più vecchio HFS (senza il "+"), in un'operazione che ricorda molto quella di FAT32 e FAT16 in ambiente Windows.
Il secondo è lo **Unix File System**, una **novità assoluta per le macchine Apple, ma uno standard del mondo Unix** e che presenta alcune particolarità tra cui quella di essere **case sensitive** e cioé di fare distinzione tra file che differiscono tra di loro semplicemente nell'uso di maiuscole o minuscole nel nome (ad es. due file chiamati "prova" e "Prova").

Sebbene sia possibile **installare OS X su una partizione UFS**, questa cosa è **sconsigliata** anche dalla Apple stessa: **la diversità di questo file system può risultare un problema** nel salvaguardare l'integrità e la coesione del data e del resource fork (le due parti di cui molti programmi e risorse Mac sono composti) proprie invece dell'HFS+, nato e cresciuto per Macintosh. **La macchina inoltre può risultare più lenta** in fase di creazione dei file, ma anche nella ricerca dei file in quanto l'UFS non permette di guardare nel "directory btree" di OSX. Infine, **il nome dell'hard disk è tassativamente "/"** come già visto nel numero 20 di Hacker Journal, pare addirittura che non sia possibile fare il boot di OSX da UFS (viene creata una mini partizione di tipo HFS+) e in passato ci sono stati anche problemi con l'ambiente "Classic" (la funzione di emulazione dei MacOS precedenti), ora risolti.

>> Cosa si può fare con l'UFS

L'UFS rappresenta un mix di vantaggi e svantaggi ed è perciò consigliato relegarlo **solo a usi come partizioni o immagini disco**, magari per lo sviluppo software o scambio dati con altri sistemi UNIX.
Per chi vuole per ora solo fare qualche esperimento, invece di avventurarsi in formattazioni o partizioni, è possibile **creare una semplice e pratica immagine disco UFS, o con il programma Disk Copy** o via Terminale con il comando "hdiutil". In questo secondo caso è addirittura possibile scegliere una modalità detta **"sparse"** con cui **la dimensione del disco virtuale non sarà fissa ma crescerà secondo necessità**, occupando quando vuota poco spazio. Ad esempio digitando

```
hdiutil create -size 1g -type
SPARSE -fs UFS ImmagineUFS
```

verrà creta un'immagine disco "ImmagineUFS" che contiene un volume logico grande fino a un giga ma che in realtà, finché è vuota, ne occupa solo una frazione, 90 Mb.

Per tutti gli altri usi **la scelta più saggia è l'HFS+** che offre stabilità e compatibilità con il passato e che con OS X 10.2.2 ha di recente anche aggiunto una interessante funzione di "journaling", simile a quelle dei filesystem EFS e VXFS di altri UNIX, a cui dedicheremo prossimamente un approfondimento.

>> Gli altri filesystem

Per quanto riguarda il "vecchio" HFS, **rimane il supporto sia in lettura che scrittura** (dischi fissi, CD-Rom, Zip, etc.) ma non è possibile usarlo per installarci su OSX, in quanto difetta della struttura per gestire nuove proprietà del sistema operativo, come i permessi.
Tra gli altri formati abbiamo già citato **UDF** e **ISO9660**: allo stesso modo è possibile leggere dischi Windows formattati come **FAT16** e **FAT32** (Windows 95, 98 e ME), anche se **non quelli NTFS**, usati da NT e ultimamente anche da Windows 2000 e XP.
È possibile inoltre **accedere ad altri periferiche in rete grazie alla presenza in OS X del protocollo SMB** (Server Message Block): SMB è l'implementazione fatta da Microsoft del CIFS (Common Internet File System) e sostanzialmente si possono raggiungere i computer Windows (e Linux) nelle reti NetBIOS selezionando la voce "Connect To Server" (command + K) dal menù "Go" nel Finder e digitando

```
smb://dominio/nome
computer/nome cartella condivisa
```

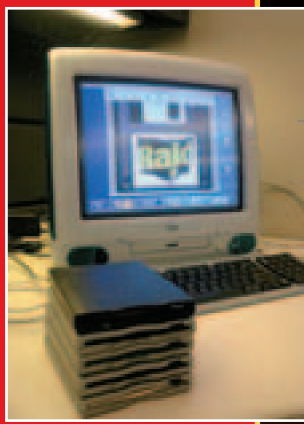
Con Mac OS X 10.2 è inoltre possibile "sfogliare" la rete senza dover usare sintassi complicate. Chi non ha fatto ancora l'upgrade a Jaguar, può scaricare "SMB Browse" (http://shukwit.com/smbbrowse.9.2.sit) utility che permette di fare lo stesso..

>> Non solo Windows: EXT2FS

È disponibile (https://sourceforge.net/projects/ext2fsx/) "Mac OS X Ext2 Filesystem" un prezioso aiuto a chi cerca di far comunicare tra di loro Linux e Mac.
Si tratta di un'implementazione fatta da del filesystem di tipo "EXT2", in genere **standard sulle distribuzioni Linux** e il suo uso, seppure sia un progetto indipendente e in fase embrionale **è perfettamente trasparente**. L'installazione del programma aggiunge un'estensione al kernel che si integra con gli altri filesystem. Non solo è possibile leggere e scrivere dischi Linux ma **funzionano anche le utility da linea di comando come "fsck".**

Nicola D'Agostino
dagostino@nezmar.com

...E I FLOPPY?



Anni fa, Apple è stata una delle prime ditte a **eliminare la presenza del drive di floppy disk** (già con il primo iMac)e di recente si sono viste anche altri produttori di compatibili muoversi nella stessa direzione.
Ciononostante sono molte le persone che usano ancora questi supporti ed esiste un mercato per i lettori esterni USB.
Anche se le performance non sono propriamente esaltanti, **i drive USB sono attualmente supportati su OSX**, fino al punto che c'è chi ha realizzato un array RAID con una catena di queste periferiche, documentando il precedimento in rete (http://ohlssonvox.8k.com/fdd_raid.htm). Meno fortunati sono coloro che hanno drive interni. Per questi esiste anche qui un progetto indipendente, chiamato SWIM e derivato da una distribuzione per Mac di Linux, che si prefigge di **far funzionare il controller dei Macintosh G3 beige** (desktop e minitower) e dei **Powerbook G3 Wallstreet e Mainstreet** (quelli neri, senza USB). Per scaricare SWIM, che è un prototipo che può anche non funzionare (come successo su un Powerbook su cui è stato provato senza successo) è disponibile all'url ftp://ftp.mklinux.org/pub/darwin/floppy/swim3-0.96.pkg.tar.gz

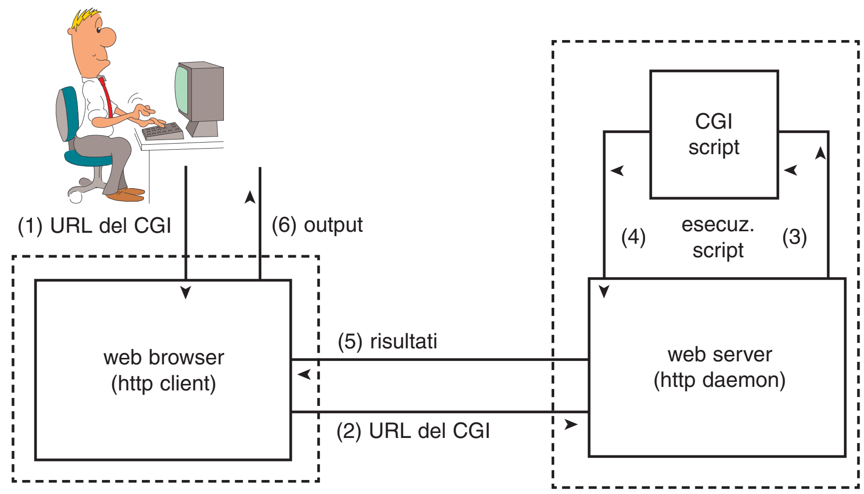
CONFIGURARE I CGI DEL WEB SERVER APACHE

PAGINE DINAMICHE

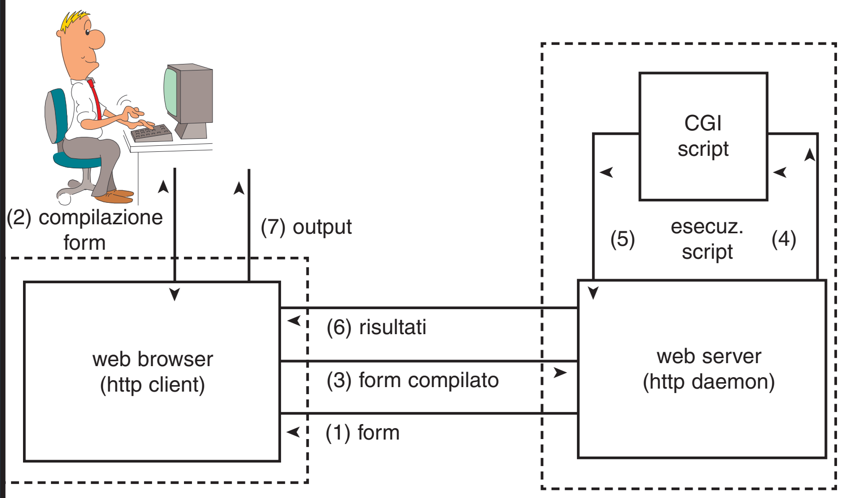
Sui numeri 23 e 24 abbiamo visto come scaricare e installare Apache su Linux, e come far partire il servizio httpd all'avvio. E' tempo ora di aggiungere qualche funzionalità in più al nostro server Web.

I CGI (Common Gateway Interface, http://hoohoo.ncsa.uiuc.edu/cgi) è uno standard per **interfacciare applicazioni esterne con un Web Server**, creando pagine HTML in modo dinamico. Tipiche applicazioni sono **query di un database** o **registrazioni di moduli compilati tramite Web,** cioè form HTML (per esempio questionari o registrazioni per accedere a qualche servizio offerto). L'applicazione CGI può essere fatto in un **qualsiasi linguaggio di programmazione che supporti delle librerie CGI** contenenti funzioni per interpretare dati mandati al Server Web tramite i metodi HTML **GET** o **POST**. I dati vengono inviati al Server Web dove c'è l'applicazione CGI installata, il quale eseguirà l'applicazione CGI interessata che genererà a sua volta un output, che il Server manderà come risposta al richiedente. Più avanti si farà un esempio che chiarirà meglio il discorso fatto.

Meccanismo CGI: attivazione diretta



Meccanismo CGI: Uso dei FORM



>> Configurare Apache per i CGI

Per poter eseguire programmi CGI, essenzialmente bisogna **impostare la directory dove sono contenuti i vari scripts**. Quando si esegue una GET/POST, per esempio nella pagina WEB da dove arriva la richiesta, si indica quasi sempre "**cgi-bin/nome_eseguibile**" dove "/cgi-bin/" è il nome simbolico (alias) che viene attribuito a tale directory. Apache quindi può essere configurato a piacere.

Aprendo il file **httpd.conf** (il noto file di configurazione) con un editor di testi, si noteranno la ripetizione di righe con prima parola la direttiva **Alias**. Questa serve per assegnare ad un nome simbolico una directory reale. In generale il comando setta le directory di sistema, per esempio con alias /icons/ si abbina la directory dove sono contenute le immagini che rappresentano le directory di files e non pagine HTML.

Per assegnare invece directory contenenti script eseguibili si usa il comando **ScriptAlias**. Detto questo se per esempio le applicazioni CGI sono nella cartella **/usr/local/apache2/cgi-bin/** si può impostare la directory così

```
ScriptAlias /cgi-bin/ "/usr/local/apache2/cgi-bin/"
```

>> Questioni di sicurezza

Con Apache è anche possibile **stabilire un comportamento particolare in base all'estensione di un file**, con il comando AddHandler. Questo comando è sconsigliato nel caso di programmi CGI, perché permetterebbe l'uso ed esecuzione di essi al di fuori della directory precedentemente settata. Quindi per questi motivi commentate (se non è già commentata) la riga:

```
#AddHandler cgi-script .cgi
```

In questo modo sistemeremo il problema per gli eseguibili che abbiano estensione .cgi, ma la cosa **si può estendere ad altri tipi di eseguibili associati ad altri tipi di script**. Sempre per questioni di sicurezza, è consigliabile **aggiungere ulteriori controlli sull'accesso alla directory**. Infatti un malintenzionato utilizzando SSI (Server Side Include, direttive che permettono all'HTML statico di essere interpretato al volo dal Server Web per inserire spezzoni di codice), potrebbe inserire in pagine Html create da lui un comando del tipo:

```
<!—#exec cgi="cgi-bin/nome_eseguibile"—>
```

Questo potrebbe permettergli di **accedere a informazioni che per noi erano da considerarsi riservate**. Per evitare questo si "blinda" la directory con una serie di direttive di sicurezza di Apache.

Normalmente l'accesso ad una directory da parte di un utente viene controllato con un file nella directory stessa, il file nascosto è **.htaccess** (il nome settato con AccessFileName); in caso di intrusioni potrebbe essere modificato e la nostra configurazione col file httpd.conf non sarebbe più valida. Per evitare questo, si usa la direttiva **AllowOverride None**, dove **None** indica che l'accesso viene controllato invece che da un file, dalle impostazioni date da questo comando (None = nessun file).

Le possibilità di configurazione sono:

None Impedisce che qualunque direttiva venga scavalcata.
All Permette che siano scavalcate tutte le direttive.
Options Permette l'uso di:
FollowSymLinks Abilita l'uso di collegamenti simbolici
SymLinksIfOwnerMatch Abilita l'uso di collegamenti simbolici solo se il proprietario coincide.
ExecCGI Permette l'esecuzione dei programmi CGI
Indexes Permette di ottenere il listato del contenuto
Includes SSI è permesso
IncludesNOEXEC SSI è permesso in parte
Limit Permette l'uso di direttive di controllo sugli accessi.
AuthConfig Permette l'uso di direttive di autorizzazione.
FileInfo Permette l'uso di direttive di controllo del tipo di documento.
Indexes Permette l'uso di direttive di controllo sul listato delle directory combinate con queste direttive

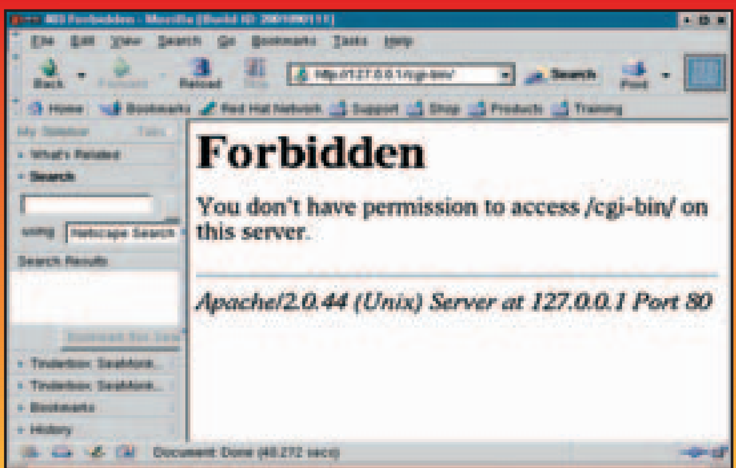
Require Utenti che possono accedere attraverso autenticazione
Deny Specifica i nodi a cui viene negato l'accesso
Allow Specifica i nodi a cui viene concesso l'accesso
Order Ordine di valutazione delle direttive deny e allow
AuthName Nome o descrizione di una zona soggetta ad autenticazione
AuthType Definizione del tipo di autenticazione.

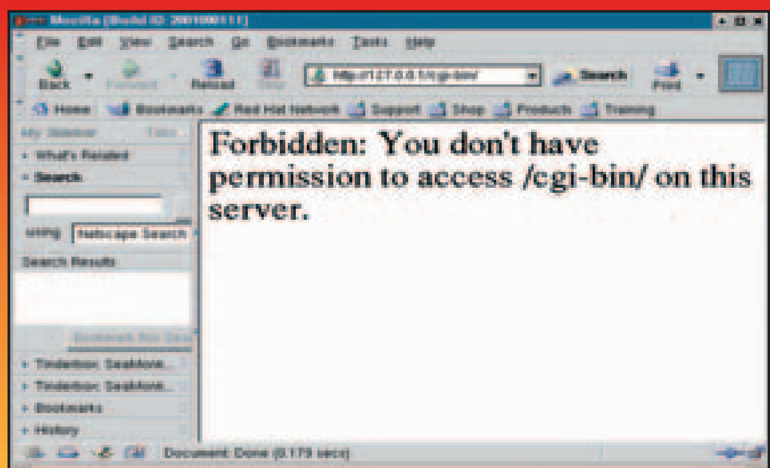
quindi si può settare la directory per gli eseguibili CGI in questo modo

```
<Directory "/usr/local/apache2/cgi-bin">
  AllowOverride None
  Options ExecCGI
  Order deny,allow
  Allow from all
</Directory>
```

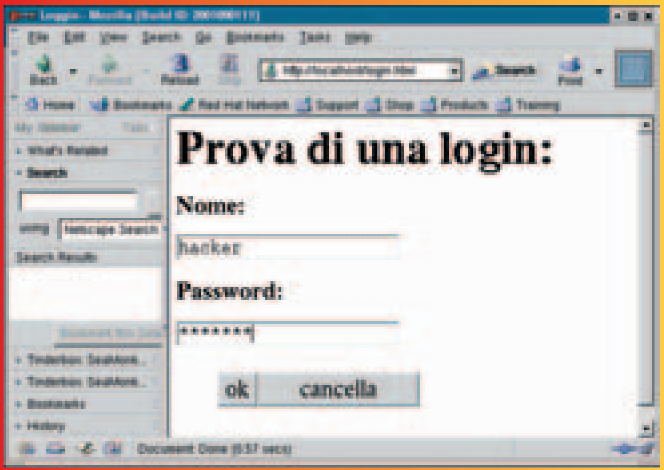
>> Gestire gli errori

L'ultima cosa da settare per motivi di sicurezza è la pagina di errore. Essa **viene generata al momento di un eventuale problema nella fase di esecuzione di un programma CGI,** oppure in una ricerca azzardata di un malintenzionato. Se da un browser viene digitata la stringa **"http://nomesito/cgi-bin/"**, normalmente viene generata una pagina di errore se l'estraneo non ha permessi di accesso. Questa pagina però **svela**

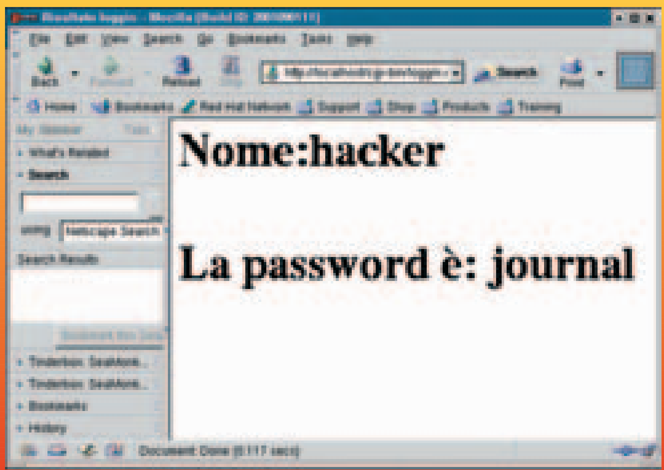




La pagina di errore standard permette di scoprire la versione del server utilizzata. Se un malintenzionato vuole scoprire questo dato, facciamolo almeno lavorare un po' di più, eliminando questa inutile informazione, con una pagina di errore personalizzata.



Una tipica pagina di autenticazione, con nome utente e password. Uno dei tanti utilizzi dei CGI.



Il risultato dell'esecuzione del CGI presentato in queste pagine.

la versione di Apache utilizzata. Sapendo la versione, un malintenzionato, potrebbe cercare eventuali bug conosciuti e non ancora sistemati dall'amministratore del sito. Quindi è sempre importante aggiornare il Server Web che si è installato. Per rendere difficile la vita dell'eventuale intrusore è consigliabile modificare la pagina in questo modo.

```
ErrorDocument 403 "Forbidden: You don't
have permission to access /cgi-bin/ on this
server."
```

infatti con la direttiva ErrorDocument e il numero dell'errore **si può settare la risposta da dare**, in formato testo o pagina html, quindi per i discorsi fatti prima si possono cambiare a piacimento le pagine di errore o crarne alcune in modo dinamico con script CGI.

```
ErrorDocument 404 /missing.html
```

Esempi di pagine di errori si possono trovare nella cartella /usr/local/apache2/error.

>> Esempio di script-CGI

Un veloce esempio di script CGI potrebbe essere l'implementazione di una pagina Web di login, che richiede l'inserimento di username e password, li passa come parametri all'applicazione CGI e come risultato produce la visualizzazione di ciò che si è introdotto. L'esempio svolto è uno script-CGI fatto in C. Normalmente questi script vengono fatti in Perl, che è un linguaggio interpretato dove la compilazione è al volo, ma come dicevamo questa non è l'unica opzione.
Partendo dal form in html si ha:

```
<html>
<head>
      <meta http-equiv="content-type"
      content="text/html; charset=ISO-8859-1">
      <title>login</title>
</head>
<body>
      <h1>Prova di una login: </h1>
      <form action="/cgi-bin/login.cgi"
       enctype="multipart/form-data"
       method="post">
      <h3> Nome: </h3><br>
      <input type="text" name="nome">
      <h3> Password: </h3>
      <input type="password" name="password">
<br>
      <input type="submit" value="ok"><input
       type="reset"value="cancella">
       </form><br>
</body>
</html>
```

Senza entrare troppo nel dettaglio (per saperne di più sull'HTML, andate su http://www.w3.org/TR/html4/) si può notare l'inizio del form (form action), notare il file eseguibile chiamato "/cgi-bin/login.cgi". Un'altra cosa da notare sono gli oggetti di input, **input type="text"** e **input type="password"**, i loro nomi sono i nomi dei parametri da verificare. Ora si dia una occhiata alllo script-cgi scritto in C, nel riquadro in queste pagine.
Inanzitutto per compilare lo script si deve possedere il file **cgic.h** (scaricabile da http://www.boutell.com/cgic) e il file **cgic.c** contenente tutte le funzioni che servono per gestire i parametri (anche per l'attivazione di eventuali cookie e altro). Ora come si può notare con la funzione **cgiFormEntries**, si controllano i parametri esistenti, in questo caso esisteranno sempre ma per altri oggetti di input (come i check box) non è detto che ci siano. Altra funzione importante è la **cgiFormString**, dal nome del parametro si ricava il valore, nella variabile result. Infine si libera la memoria allocata nella variabile array (usata per il controllo dei parametri) con la funzione **cgiStringArrayFree**. Si può notare, in base ai parametri introdotti, la stampa sullo standard output **cgiOut** usando la funzione **printf**. Apache invierà il tutto al browser client richiedente. La funzione **cgiHeaderContentType**, me-

no importante delle altre, mette come intestazione di risposta lo stesso header della pagina richiedente.
Per compilare il file C, chiamato per esempio **login.cgi.c** , se si desidera che crei il file eseguibile login.cgi nella directory con il file cgic.c e cgic.h, si deve eseguire il comando da shell

```
gcc -o login.cgi login.cgi.c cgic.c
```

Ora, conservando i file sorgenti in un posto sicuro, va copiato il file eseguibile **login.cgi** nella directory **/usr/local/apache2/cgi-bin**. La pagina Web HTML la si può creare copiando il testo descritto sopra in un nuovo file di testo, rinominarlo come file .html per esempio, e copiarlo all'interno della directory delle pagine HTML del Server Web. Con un browser provare a visualizzare la pagina e vederne il funzionamento.

boymix81@libero.it

IL CODICE DEL CGI

```
#include <stdio.h>
#include "cgic.h"
#include <string.h>
#include <stdlib.h>

void HandleSubmit();
void ShowForm();
void CookieSet();
void Name();
void Address();
void Hungry();
void Temperature();
void Frogs();
void Color();
void Flavors();
void NonExButtons();
void RadioButtons();
void File();
void Entries();
void Cookies();
void LoadEnvironment();
void SaveEnvironment();

int cgiMain() {
      char **array;
      char result[256];
      /* riscrivi come header lo stesso della pagina di richiesta*/
      cgiHeaderContentType("text/html");

      /*titolo pagina*/
      fprintf(cgiOut, "<HTML><HEAD>\n");
      fprintf(cgiOut, "<TITLE>Risultato login:</TITLE></HEAD>\n");

      /* verifica del corretto passaggio dei parametri */
      if (cgiFormEntries(&array) != cgiFormSuccess) { return 0; }

      /* elaborazione parametri ( stampo solo ) */
      cgiFormString("nome",result,256);
      if (strlen(result)==0)
      fprintf(cgiOut, "<BODY><H1>Manca il nome</H1><br>");
      else
      fprintf(cgiOut, "<BODY><H1>Nome:%s</H1><br>",result);
      cgiFormString("password",result,256);
      if (strlen(result)==0)
      fprintf(cgiOut, "<BODY><H1>Manca la password</H1><br>");
      else
      fprintf(cgiOut,"<BODY><H1>La password è:%s</H1><br>",result);

      /* CHIUSURA CODICE HTML */
      cgiStringArrayFree(array);
      fprintf(cgiOut, "</BODY></HTML>\n");
      return 0;
      }
```



COME USARE LA PIATTAFORMA DI SVILUPPO JAVA

Java: COMINCIAMO A PROGRAMMARE

Per assaporare meglio il linguaggio Java occorre conoscere bene l'ambiente di sviluppo col quale programmiamo ed utilizzare al meglio tutti gli strumenti che i ricercatori della Sun ci mettono a disposizione.

Abbiamo già avuto modo di dire che per scrivere, compilare ed eseguire codice Java non è necessario districarsi tra vari comandi che possono confondere le idee a chi ancora non ha dimestichezza con il mondo della programmazione. È infatti necessario lanciare il comando javac per compilare il nostro codice ed in seguito il comando java per eseguirlo. Ma si sa, **uno smanettone non si accontenta di conoscere lo stretto indispensabile delle cose...**

>> Da dove inizio?

Per iniziare ovviamente è necessario scaricare il software di sviluppo. Dal sito ufficiale di Java, http://java.sun.com/j2se è possibile scaricare la piattaforma standard edition. Qui troviamo due differenti pacchetti da scaricare: **JRE** ed **SDK**. Il primo comprende il **Java Runtime Environment,** ovvero il runtime del linguaggio, costituito dalla macchina virtuale e dai pacchetti base della piattaforma. Questa distribuzione è rivolta soltanto agli utenti e non agli sviluppatori. **Per iniziare a scrivere o modificare programmi in Java dobbiamo utilizzare il Software Development Kit, o JDK**, che comunque al suo interno comprende anche il pacchetto JRE. Parecchie piattaforme supportano la tecnologia Java. Sul sito ufficiale troviamo la piattaforma di sviluppo per Windows, Linux e Solaris. Altri sistemi operativi sono supportati da terze parti. Ad esempio, se volete programmare in Java sotto Mac OS, potete reperire informazione su www.apple.com/java o su http://developer.apple.com

>> Cosa contiene

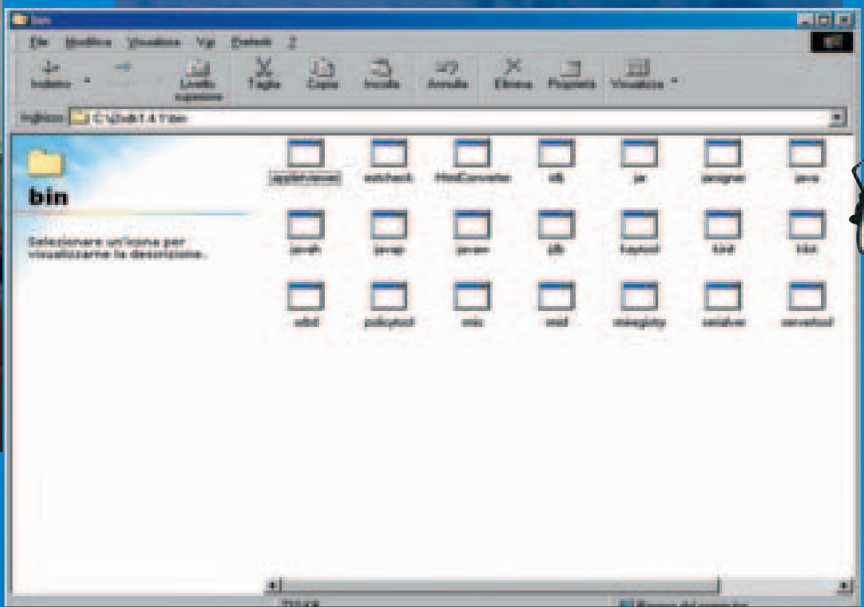
La distribuzione standard dell'ambiente di sviluppo è divisa in tre parti:

Strumenti di sviluppo: A questa categoria appartengono tutti gli strumenti che ci permettono non soltanto di compilare ed eseguire il codice Java, ma anche altri **software utili per la verifica e la distribuzione del bytecode prodotto**. Troviamo questi strumenti all'interno della cartella bin dopo avere installato l' ambiente di sviluppo. Tra gli strumenti più interessanti troviamo **l'appletviewer,** che ci consente di visualizzare e testare le nostre applet prima di inserirle in una pagina HTML e il **jar**, grazie al quale possiamo racchiudere un programma scritto in Java in un file compresso JAR. Questi archivi oltre che garantire una maggiore facilità di distribuzione del software, possono rendere il software da noi realizzato eseguibile senza utilizzare la riga di comando.



Applet Sono delle applicazioni scritte interamente in Java che vengono caricate dal browser come parte integrante di una pagina HTML.

Macchina Virtuale: Questo componente è necessario per l'esecuzione del bytecode. Installando l'SDK avremo a disposizione anche la macchina virtuale Java.
Pacchetti base: Possiamo pensare ai pacchetti come a delle raccolte di funzionalità software che soddisfano le esigenze più svariate dei programmatori Java. All'interno dei pacchetti base, quindi, saranno contenuti **strumenti utili per il networking, per la manipolazione delle immagini o per l'utilizzo di date ed orari**, per esempio.



Aprendo la cartella bin dell'sdk possiamo vedere tutte le applicazione che ci permetto di gestire al meglio il nostro codice scritto in Java.

>> Java e windows

Per installare la piattaforma J2sdk su Windows è necessario semplicemente avviare il programma di installazione. Dobbiamo spendere invece due parole sulla sua configurazione, che **se eseguita in modo errato, a volte può complicarci la vita...** Annotando il percorso degli eseguibili nella variabile di sistema PATH, infatti richiameremo tutto ciò che ci serve per programmare senza dovere scrivere da riga di comando l'interno percorso nel quale sono situati gli eseguibili della cartella bin. Nel caso in cui avete eseguito l'installazione standard dell'SDK 1.4.1 su Windows 95 e 98 occorre **aggiungere la seguente riga al file Autoexec.bat**:

```
SET PATH=%PATH%; C:\j2sdk1.4.1\bin
```

In Windows XP e 2000 invece dovete accedere alla voce **Sistema -> Avanzate -> Variabili d'ambiente**. A questo punto dobbiamo modificare la voce PATH, aggiungendo nel campo valore il percorso

```
C:\j2sdk1.4.1\bin
```

Ovviamente per eseguire questa operazione è necessario avere i diritti di amministrazione sul sistema.

JAR È un archivio compresso contenente codice Java che può essere reso avviabile come un normale file EXE.

>> Java e Linux

Per Linux, come abbiamo avuto già modo di sottolineare, **sono disponibili due SDK**. Benché Sun Microsystems supporti soltanto Linux Red Hat è possibile installare l'ambiente di sviluppo sulla maggior parte delle distro. Il nome del file RPM è j2sdk-1_4_1-linux-i386-rpm.bin (ovviamente può cambiare il numero di versione e di conseguenza anche il nome del file da scaricare). **Per avviare l'installazione, da root digitiamo**:

```
rpm –iv j2sdk-1_4_1-fcs-linux-i386.rpm
```

Il secondo file disponibile per il download prende il nome di Linux GNUZIP. Per installarlo **posizioniamo il file in una directory qualsiasi e poi lanciamo il comando**

```
./j2sdk-1_4_1-linux-i386.bin
```

Anche in questo caso aggiungiamo alla variabile di sistema PATH il percorso che ci indica dove sono situati gli eseguibili dell'SDK Supponendo che abbiamo installato tutto all'interno della directory /usr/java/j2sdk1.4.1 occorre aggiungere la seguente riga al file /etc/profile, agendo come root

```
PATH="$PATH:/usr/java/j2sdk1.4.1/bin"
```

Bene, adesso che abbiamo installato la piattaforma di sviluppo vediamo come utilizzare al meglio i suoi strumenti più importanti.

Il sito www.apple.com/java/, dal quale potrete scaricare tutto il necessario per programmare in Java sul vostro Mac OS.





Download J2SE v 1.4.1_02	JRE	SDK
Windows (U.S. English only)	DOWNLOAD	N/A
Windows (all languages, including English)	DOWNLOAD	DOWNLOAD
Linux RPM in self-extracting file	DOWNLOAD	DOWNLOAD
Linux self-extracting file	DOWNLOAD	DOWNLOAD
Solaris SPARC 32-bit self-extracting file	DOWNLOAD	DOWNLOAD
Solaris SPARC 32-bit packages - tar.Z	N/A	DOWNLOAD
Solaris SPARC 64-bit self-extracting file*	DOWNLOAD	DOWNLOAD
Solaris SPARC 64-bit packages - tar.Z*	N/A	DOWNLOAD
Solaris x86 self-extracting file	DOWNLOAD	DOWNLOAD
Solaris x86 packages - tar.Z	N/A	DOWNLOAD
Installation Instructions	VIEW	VIEW
ReadMe	VIEW	VIEW
Release Notes	VIEW	VIEW
License for all platforms	VIEW	VIEW

* Solaris 64-bit requires users to first install 32-bit

Queste sono le versione di j2sdk scaricabili gratuitamente dal sito ufficiale di Sun Microsystems.

>> Il compilatore



Il compilatore è uno degli strumenti essenziali della piattaforma si sviluppo in quanto **converte il nostro sorgente che avrà estensione .java in bytecode**, il codice già compilato che poi sarà eseguito dalla Java Virtual Macchine. Parlando del compilatore è bene sottolineare che oltre al compilatore di Sun Microsystems ne esistono altri. Uno dei migliori, **Jikes**, è stato prodotto direttamente da IBM. Questo prodotto è leggerissimo e la sua natura open source ha spinto alcuni programmatori a realizzare il porting verso altri sistemi non supportati direttamente da IBM. Oltre che per **Linux, Windows e Mac OS** è stata realizzata una **versione di Jikes per sistemi Amiga**. Il comando da utilizzare per compilare un file sorgente è il seguente:

```
javac nome_della_classe.java
```

Ogni programma scritto in Java sarà costituito da una serie di classi che dipendono l'una dall'altra. Quando si compila un programma non si dovranno compilare tutte le classi che fanno parte di quel software in quanto **il compilatore rileva automaticamente le dipendenze tra i vari file**. Quando vogliamo compilare tutti i sorgenti contenuti in una directory, possiamo spostarci nella directory che ci interessa e digitare:

```
javac *.java
```

Così facendo, tutti i file con estensione .java saranno convertiti in bytecode. Il compilatore della Sun inoltre supporta alcune opzioni, vediamo assieme quali sono quelle più utilizzate:

javac — o nomeFile.java

IL NOSTRO PRIMO PROGRAMMA

Bene, adesso che abbiamo preso confidenza con l'ambiente di lavoro, non ci resta che cominciare a smanettare con un po' di codice… Questa volta cominciamo con qualcosa di leggermente più complesso dell'ormai noto programma che ci dice "Hello World". Nell'esempio da me commentato potete vedere come con poche righe di codice possiamo crearci un "rudimentale" orologio virtuale. Vi invito pertanto a cominciare da questo esempio e magari di provare a migliorarlo…

```
// Importiamo java.util.Date per la manipolazione di date e orari
 import java.util.Date;

// Definiamo la classe chiamandola data
 class data {

// Introduciamo il metodo main()
  public static void main(String[] args) {

//Creiamo un nuovo oggetto di tipo Date
   Date data = new Date() ;

// Utilizzando i metodi getHours() e getMinutes() facciamo stampare a video l'ora corrente
   System.out.println(" Sono le ore: "+data.getHours()
                         +":" +data.getMinutes());
      }
}
```



Utilizzando questa opzione il bytecode prodotto avrà prestazioni più elevate. L'utilizzo del parametro — o è consigliato per la pubblicazione finale del software che vogliamo realizzare.

javac — g nomeFile.java
Con questa opzione il compilatore include nel bytecode alcune informazioni che ci potranno essere utili nella fase di debug del nostro programma. Infatti in caso di errore avremo un quadro dettagliato del problema quando eseguiamo il nostro bytecode.

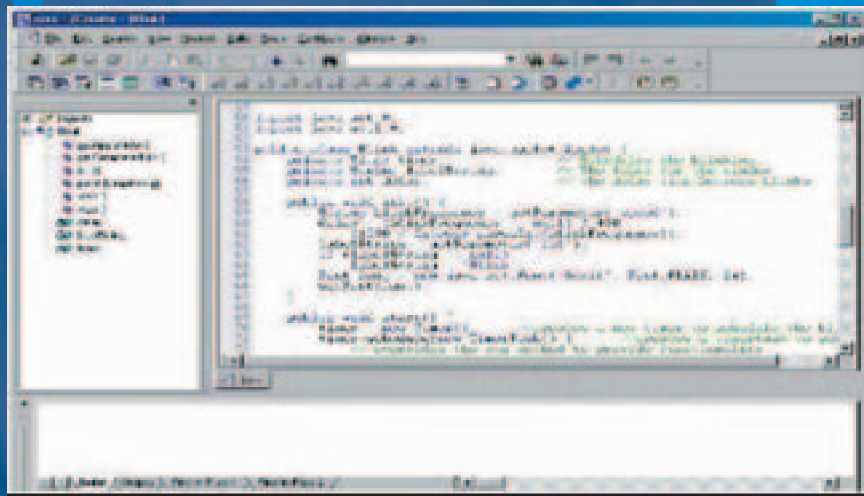
javac @nomeFile.txt
In questo modo possiamo conservare tutti gli argomenti che dovremmo passare manualmente al compilatore in un file di testo e poi richiamare questo file utilizzando questa opzione. Supponiamo per esempio che vogliamo compilare i file HackerJournal.java e CiaoMondo.java utilizzando le opzioni — o e — g. Creiamo il file di testo SorgentiJava.txt e digitiamo su righe distinte:

```
-     o
-     g
HackerJournal.java
CiaoMondo.java
```

Poniamo il file di testo nella stessa directory contenente i file sorgente e lanciamo il comando

javac @SorgentiJava.txt

Otterremo lo stesso risultato che si avrebbe digitando i singoli argomenti da riga di comando.



Utilizzando un editor facilitato, come Jcreator, è possibile scrivere il nostro codice e testarlo attraverso una comoda interfaccia grafica.



>> L'interprete

Per eseguire le applicazioni java dobbiamo necessariamente utilizzare l'interprete o esecutore. Il comando che utilizzeremo per avviare l'interprete è il seguente

```
java nomeClasse
```

senza specificare l'estensione del bytecode (.class). L'interprete esegue solo file che rappresentano un'applicazione, e che quindi contengono il metodo statico main(). Ovviamente anche l'interprete supporta alcune opzioni. Come sempre vediamo assieme quelle più utilizzate:

java —version
Utilizzando questa opzione saranno visualizzate alcune informazione che riguardano l'ambiente di sviluppo da noi utilizziamo ed il suo numero di versione

java —classpath
Con l'opzione classpath specificheremo il percorso nel quale si trovano i nostri file class.

java — client
Con il parametro -client verrà ottimizzata l'esecuzione per programmi di natura client in sistemi Windows. Per avere lo stesso risultato quando lavoriamo con sistemi Linux l'opzione da utilizzare sarà **— hotspot.**

java —server
Questa opzione ottimizza l'esecuzione per programmi di natura server.

Ricordiamo comunque che il comando **java** non è l'unico in grado di eseguire le nostre applicazioni. All'interno della cartella bin di J2sdk troviamo l'applicazione **javaw**, che sui sistemi Windows permette l'esecuzione di applicazioni a finestre senza tenere impegnata nello stesso tempo la nostra console.

Nel prossimo numero vedremo come realizzare le nostre prime applicazioni interamente in Java

Antonino Benfante

LINK UTILI

Sito ufficiale di Sun Microsystems
http://java.sun.com

Qui potete trovare tutto per programmare sotto Mac OS
http://www.apple.com/java
http://developer.apple.com/java

Sito ufficiale di Jikes, il compilatore open source di IBM
http://ibm.com/developerworks/opensource/jikes/

Da questo indirizzo potete scaricare un'ottimo editor facilitato per Windows completamente gratuito ed efficiente
http://www.jcreator.com/